Bundesministerium
des Innern

Schutz Kritischer Infrastrukturen – Basisschutzkonzept

Empfehlungen für Unternehmen

www.bmi.bund.de

Vorwort

Infrastrukturen haben in unseren Gesellschaften die Funktion von Lebensadern. Wir sind darauf angewiesen, dass die Versorgung mit Energie und Wasser, mit Informationstechnik und Mobilität zuverlässig funktioniert. Fallen diese Systeme oder andere wichtige Infrastrukturen auch nur für kurze Zeit in größerem Umfang aus, so kann dies schwerwiegende Folgen haben.

In besonderem Maße haben die Anschläge in New York und Washington am 11. September 2001, in Madrid am 11. März 2004 und in London am 7. und 21. Juli 2005 die Gefährdung offener Gesellschaften gezeigt. Die Bekämpfung des internationalen Terrorismus und der Schutz der Bevölkerung vor dieser Bedrohung erfordern daher die besondere Aufmerksamkeit der Sicherheitsbehörden.

Neben der Abwehr terroristischer Anschläge gilt es auch, andere Gefährdungen ins Blickfeld zu nehmen. So können Naturkatastrophen wie zum Beispiel Überschwemmungen erhebliche Zerstörungen nach sich ziehen.

Der Schutz so genannter Kritischer Infrastrukturen – also von Einrichtungen und Organisationen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden – ist umfassend anzugehen. Daher ist es richtig, dass Staat und Wirtschaft den Dialog über dieses Thema verstärken und gemeinsam Lösungen für mehr Sicherheit entwickeln.

Als einen Beitrag dazu haben das Bundesministerium des Innern, das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe und das Bundeskriminalamt ein Basisschutzkonzept erarbeitet. Von Beginn an wurde dieses Vorhaben durch Sachverstand aus der Wirtschaft begleitet und vorangebracht. Für diese Unterstützung dankt das Bundesministerium des Innern den Sicherheitsbeauftragten

- der Deutschen Bahn AG, Herrn Jens Puls,
- der DFS, Deutsche Flugsicherung GmbH, Herrn Hans-Jürgen Morscheck,
- der Deutz AG, Herrn Werner Becker,
- der IBM Deutschland GmbH, Herrn Klaus Hintz,
- der Vattenfall Europe Transmission GmbH, Herrn Thomas Schäfer

und ihren Mitarbeiterinnen und Mitarbeitern.

Mit dem Basisschutzkonzept liegen für die Unternehmen in Deutschland Empfehlungen aus dem Blickwinkel der Inneren Sicherheit vor. Die hohe Sicherheit der Infrastrukturen ist ein herausgehobenes Qualitätsmerkmal Deutschlands. Dieses auch langfristig abzusichern, liegt im elementaren Interesse der Unternehmen und der Bürgerinnen und Bürger unseres Landes.

Berlin, August 2005

Die Bahn DB DFS Deutsche Flugsicherung DEUTZ SICHERHEIT IBM VATTENFALL

Inhalt

Zusammenfassung

Ziel des vorliegenden Basisschutzkonzeptes ist die Reduzierung der Verwundbarkeit Kritischer Infrastrukturen gegenüber natürlichen Ereignissen und Unfällen sowie gegenüber terroristischen Anschlägen und kriminellen Handlungen. Das Basisschutzkonzept fokussiert dabei auf bauliche, organisatorische, personenbezogene und technische Schutzmaßnahmen.

Anknüpfungspunkt Risikomanagement

Der Bedarf für ein Basisschutzkonzept ergibt sich unter anderem aus gesetzlichen Vorschriften und allgemein anerkannten Standards[1], aber auch aus allgemein anerkannten unternehmerischen Prinzipien eines vorausschauenden Risikomanagements und einer strategischen, auf Erfolg und Kontinuität ausgerichteten Unternehmensplanung, beispielsweise im Rahmen des so genannten Business Continuity Managements (BCM).

Adressat: Unternehmensleitung

Adressaten für die Entwicklung strategischer Konzepte für Gefährdungsanalysen, für Risikomanagementsysteme sowie von Maßnahmen zur Risikominimierung sind zunächst die Unternehmensleitungen der Infrastrukturbetreiber, die bei Verstößen das unternehmerische Risiko und auch mögliche Haftungsrisiken tragen sollten. Für die Umsetzung dieser strategischen Konzepte im Unternehmen sind die Ansprechpartner dann in aller Regel die Sicherheitsverantwortlichen. Letztlich handelt es sich bei der Umsetzung des Basisschutzkonzeptes um eine gesamtunternehmerische Aufgabe, die der Unterstützung aller Ebenen bedarf.

Voraussetzung für die Konkretisierung umfassender Schutzmaßnahmen ist eine vertrauensvolle Zusammenarbeit zwischen Staat und Infrastrukturbetreibern. Die Betreiber sind diejenigen, die über hinreichende Detailkenntnisse ihrer Infrastrukturen verfügen und konkrete Schutzmaßnahmen effektiv umsetzen können. Zunächst ist es daher nötig, sich darüber zu verständigen, welches Schutzniveau gewollt beziehungsweise akzeptabel ist.

Analyse-/ Planungsprozess

Ausgangspunkt ist ein mehrstufiger Analyse- und Planungsprozess, der eine Ermittlung der Risiken und eine daran anknüpfende Überprüfung sowie gegebenenfalls Anpassung von Schutzmaßnahmen umfasst. Er lässt sich wie folgt gliedern:

I. Die Bildung von Gefährdungskategorien, differenziert nach den Bereichen Naturkatastrophen, Unfälle, Terrorismus und Kriminalität,

II. darauf basierend die Festlegung des jeweiligen Schutzniveaus,

III. die Entwicklung von Schadens- und Bedrohungsszenarien,

IV. die Analyse von Schwachstellen,

[1] Beispielsweise aus § 91 Aktiengesetz (Aufbau von Risikomanagement- und Überwachungssystemen), aus der Störfallverordnung, aus weiteren allgemeinen und speziellen Betreiberpflichten und fachgesetzlichen Regelungen oder auch aus der neuen Eigenkapitalvereinbarung „Basel II“.

V. die Formulierung von Schutzzielen und daraus abgeleitet die Darlegung von Schutz- und Gegenmaßnahmen,

VI. die Formulierung des jeweiligen Handlungsbedarfs (Abstimmung zwischen staatlichen und privaten Maßnahmen),

VII. die Umsetzung des formulierten Handlungsbedarfs und

VIII. die regelmäßige Überprüfung dieses Analyse- und Planungsprozesses im Rahmen des Qualitätsmanagements.

Als erste Orientierungsgrundlage werden mögliche Gefährdungen für Kritische Infrastrukturen aufgezeigt. Dazu gehören im Wesentlichen Gefährdungen durch natürliche Ereignisse, menschliches oder technisches Versagen und Terrorismus beziehungsweise kriminelle Handlungen. Anhand dieser Gefährdungen können besonders gefährdete Bereiche im Unternehmen identifiziert und generalisierte Basisschutzempfehlungen abgeleitet werden.

Dort, wo dieser Prozess aufgrund fehlender Ressourcen als zu aufwändig oder nur schwer umsetzbar empfunden wird, wie zum Beispiel in kleinen und mittleren Unternehmen (KMU), kann es durchaus sinnvoll sein, sich dem Thema in kleinen Schritten zu nähern und zunächst einzelne, als besonders dringlich empfundene Aspekte des Basisschutzkonzeptes anzugehen.

Fragenkatalog/ Checkliste

Als Hilfestellung für die Umsetzung des Basisschutzkonzeptes wurden ein Fragenkatalog und eine Checkliste (Anhang 1) entwickelt, mit denen die Betreiber von Infrastruktureinrichtungen arbeiten können. Der Fragenkatalog und die Checkliste sollen als übergreifende Instrumente vor allem dazu dienen, einen unternehmensinternen Diskussionsprozess über die Erhöhung der Sicherheit zu initiieren und zielgerichtet zu steuern. Aus der Tatsache, dass es sich sowohl beim Fragenkatalog als auch bei der Checkliste nicht um abschließende Kataloge, sondern lediglich um Muster handeln kann, folgt, dass fehlende Punkte im Rahmen dieses Prozesses ergänzt werden müssen oder nicht zielführende Fragen modifiziert oder gestrichen werden können.

Ziel dieses Entwicklungsschrittes ist es, aus dem Blickwinkel der Inneren Sicherheit und in enger Diskussion mit Staat und Betreibern von Infrastruktureinrichtungen gemeinsam Prioritäten zu setzen und Maßnahmen zum Schutz Kritischer Infrastrukturen zu operationalisieren.

Ansprechpartner zum Basisschutzkonzept:
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe
Zentrum Schutz Kritischer Infrastrukturen
Deutschherrenstraße 93–95
53177 Bonn
BBK-Zentrum-I@bbk.bund.de
http://www.bbk.bund.de

Bundeskriminalamt
65173 Wiesbaden
http://www.bka.de oder http://www.bundeskriminalamt.de

1 Zielsetzung
und methodische Grundlagen

Ausgehend von der Betrachtung möglicher Gefährdungen durch Naturkatastrophen, durch Ereignisse technischen oder menschlichen Versagens, durch Terrorismus oder kriminelle Handlungen erscheinen Maßnahmen zur Grundsicherung unserer hochkomplexen wirtschaftlichen und gesellschaftlichen Infrastrukturen zwingend erforderlich – insbesondere, wenn es sich um Infrastrukturen „mit wichtiger Bedeutung für das staatliche Gemeinwesen (handelt), bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden".[2] Für diese so genannten Kritischen Infrastrukturen sind Maßnahmen zur Schadensbegrenzung und -bewältigung, aber vor allem auch präventive Maßnahmen vorzuhalten und zu entwickeln, mit deren Hilfe das Entstehen erheblicher Störungen von vornherein vermieden oder zumindest deren Folgen so gering wie möglich gehalten werden können.

Definition KRITIS

Basis: Kooperation Staat/Wirtschaft

Voraussetzung für die Konkretisierung und Formulierung von notwendigen Schutzmaßnahmen ist eine vertrauensvolle Kooperation zwischen Staat und Betreibern von Infrastruktureinrichtungen: Während der Staat weiterhin Garant für die Innere Sicherheit ist und auch Informations- und Kommunikationsprozesse moderiert, verfügen die Betreiber über hinreichende Detailkenntnisse ihrer Infrastrukturen, so dass konkrete Schutzmaßnahmen nur von ihnen selbst effektiv umgesetzt werden können.

Anknüpfungspunkte für ein Basisschutzkonzept ergeben sich zum einen aus gesetzlichen Vorschriften, zum anderen aus allgemein anerkannten unternehmerischen Prinzipien eines vorausschauenden Risikomanagements und einer strategischen, auf Erfolg und Kontinuität ausgerichteten Unternehmensplanung (zum Beispiel im Rahmen des so genannten Business Continuity Managements – BCM).

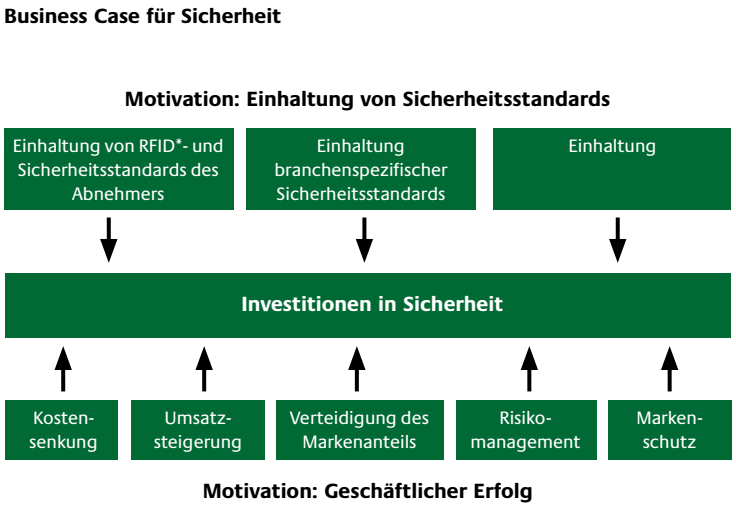
Risikomanagement, Betreiberpflichten, Fachgesetze

So besteht für eine Reihe von Betreibern die Verpflichtung des Vorstandes nach § 91 Absatz 2 Aktiengesetz (AktG), geeignete Maßnahmen zu treffen und Überwachungssysteme – etwa ein Risikomanagementsystem – aufzubauen, um die den Fortbestand der Gesellschaft gefährdenden Entwicklungen früh zu erkennen. Zu derartigen Entwicklungen zählen neben risikobehafteten Geschäften und Verstößen gegen gesetzliche Vorschriften auch Gefährdungen durch Naturereignisse oder Terrorakte, die erheblichen Einfluss auf den Fortbestand der Unternehmung haben können. Nicht zuletzt mit der Eigenkapitalvereinbarung „Basel II" und den beschlossenen Standards zur Vergabe von Krediten treten Fragen der Einschätzung und Bewertung unternehmerischer Risiken stärker in den Vordergrund.

Ein weiterer Anknüpfungspunkt für Maßnahmen zum Schutz Kritischer Infrastrukturen ergibt sich aus der Verantwortung der Betreiber, ihre Anlagen gegenüber möglichen Gefahren zu sichern und die erforderlichen Vorkehrungen zu treffen. Diese Betreiberpflichten sind zum Teil gesetzlich geregelt (allgemeine Betreiberpflichten und spezifische, etwa nach dem Telekommunikationsgesetz, der Gefahrgutverordnung oder für Betriebe, die der Störfallverordnung unterliegen). Zum Teil sind sie aber auch Bestandteil allgemein anerkannter unternehmerischer Grundsätze, wie sie zum Beispiel die Grundsätze ordnungsgemäßer Unternehmensführung und -leitung darstellen. Hinzu kommen allgemeine und fachspezifische gesetzliche Regelungen, zu denen etwa Feuer- und Brandschutzgesetze, das Bauordnungs- und Planungsrecht, aber auch das Umwelt- oder Energiewirtschaftsrecht zählen.

[2] Definition Kritischer Infrastrukturen des AK KRITIS im Bundesministerium des Innern (BMI) vom 17.11.2003.

Abbildung 1: Motivation für Sicherheit in Unternehmen



* Technologien wie RFID (Radio Frequency Identification), Sensoren, intelligente Container sowie Softwarelösungen für Reporting und Supply Chain Management können in Kombination mit optimierten Verfahren und Abläufen die Lieferkette deutlich übersichtlicher machen.

Abbildung und Erläuterung nach: Deloitte, Erfolg in der Secure Economy – Wachstum und Wohlstand in einer sicheren Wirtschaft. Executive Summary, 2004, S. 4 f.

Maßnahmen gegen Eingriffe Unbefugter

Unter dem Gesichtspunkt der Sicherheit stellen insbesondere Maßnahmen gegen Eingriffe Unbefugter einen wichtigen Beitrag zum Schutz Kritischer Infrastrukturen dar. Einrichtungen sollen derart gegen durch Vorsatz und durch natürliche Ereignisse oder Unfälle ausgelöste Störungen gesichert sein, dass eine ernste Gefahr, beispielsweise durch Explosion oder Ausbreitung gefährlicher Stoffe, möglichst ausgeschlossen werden kann. Auch ein Ausfall der bereitgestellten Produkte und Dienstleistungen muss vermieden werden, sofern hieraus erhebliche Gefahren im Sinne der eingangs genannten KRITIS-Definition erwachsen können.

Ziel: Reduzierung der Verwundbarkeit

Wichtigstes Anliegen des Basisschutzkonzeptes ist der Schutz menschlichen Lebens durch Reduzierung der Verwundbarkeit Kritischer Infrastrukturen gegenüber natürlichen Ereignissen, gegenüber Ereignissen aufgrund technischen oder menschlichen Versagens sowie gegenüber terroristischen Anschlägen und kriminellen Handlungen. Das Basisschutzkonzept soll bauliche, organisatorische, personenbezogene und technische Standard-Sicherheitsmaßnahmen berücksichtigen.

Was das Basisschutzkonzept nicht berücksichtigt

Wenngleich auch Gefährdungen der Umwelt eine gravierende Bedrohung darstellen können, werden im Sinne eines pragmatischen Vorgehens reine Umweltauswirkungen in diesem Konzept nicht spezifisch behandelt. Es kann hierfür aber sinngemäß die gleiche Vorgehensweise angewendet werden. Kriminelle Angriffe auf Unternehmen, die vor allem deren Wettbewerbsfähigkeit schädigen, wie zum Beispiel Industriespionage, werden ebenfalls nicht betrachtet.

Nicht Gegenstand der nachfolgenden Betrachtungen sind schließlich auch außerbetriebliche Gefahrguttransporte. Grundsätzlich gilt aber, dass für Gefahrguttransporte ähnliche Sicherungsüberlegungen anzustellen sind, wie sie hier für die stationären Anlagen angestellt werden. Zu- und Abgangswege und insbesondere deren Sicherung müssen im Einzelfall auf Schnittstellen mit dem Transportwesen untersucht und behandelt werden. Für die Entwendung von Gefahrstoffen und deren vorsätzlichen Missbrauch sind ebenfalls gesonderte Überlegungen anzustellen.

Auch Angriffe über die elektronische Vernetzung der Unternehmen („Cyberattacken“) sind von Bedeutung. Da sich das Basisschutzkonzept jedoch auf die Abwehr physischer Gefährdungen konzentriert, wird hinsichtlich der IT-Sicherheit auf bestehende Konzepte wie beispielsweise die ISO-Norm 17799 sowie das IT-Grundschutzhandbuch und die weiteren Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verwiesen.

Analyse-/ Planungsprozess

Um zu tragfähigen und letztlich umsetzbaren Aussagen zu gelangen, muss grundsätzliches Einvernehmen darüber erreicht werden, welches Schutzniveau gewollt und akzeptabel ist. Zur Entwicklung des Schutzkonzeptes ist daher folgendes systematisches Vorgehen angezeigt:

I. Die Bildung von Gefährdungskategorien, differenziert nach den Bereichen Naturkatastrophen, Ereignisse technischen oder menschlichen Versagens sowie Terrorismus und kriminelle Handlungen,

II. darauf basierend die Festlegung des jeweiligen Schutzniveaus,

III. die Entwicklung von Schadens- und Bedrohungsszenarien,

IV. die Analyse von Schwachstellen,

V. die Formulierung von Schutzzielen und daraus abgeleitet die Darlegung von Schutz- und Gegenmaßnahmen,

VI. die Formulierung des jeweiligen Handlungsbedarfs (Abstimmung zwischen staatlichen und privaten Maßnahmen),

VII. die Umsetzung des formulierten Handlungsbedarfs und

VIII. die regelmäßige Überprüfung dieses Analyse- und Planungsprozesses im Rahmen des Qualitätsmanagements.

Kompetent und verantwortlich für die Umsetzung von Maßnahmen zur Realisierung des Basisschutzkonzeptes sind die Betreiber. Zu analysieren sind in diesem Zusammenhang unter anderem folgende Aspekte:[3]

- Beurteilung der Gefährdungslage (allgemeine Sicherheitslage, Größe und Zusammensetzung der Belegschaft, Qualität der Sicherheitsorganisation, gesellschaftliche Position von Angehörigen der Unternehmensleitung, Art der Vertriebsverbindungen und Auslandsaktivitäten, bisher festgestellte Kriminalität etc.),
- örtliche Lage des Betriebsbereichs und der Anlagen (Verwundbarkeit von außen und innen, Entfernung zum Werkszaun, Einsehbarkeit von außen, Verkehrswegeführung innen und außen, Nähe zu anderen Industriebereichen oder Kritischen Infrastrukturen, geologische [zum Beispiel Erdbebengefährdung] und geographische [zum Beispiel Flussnähe, Topographie] Gegebenheiten),
- Bedeutung der Anlagen für vor- und nachgelagerte Produktionsprozesse und Dienstleistungen (zum Beispiel wirtschaftliche Schäden, Produktions- und Lieferausfälle),
- Symbolcharakter der Unternehmung beziehungsweise Anlagen (Art der Produktion und der Lagerung von Stoffen, Produktpalette, wirtschaftlich-strategische Bedeutung des Unternehmens),
- Interdependenzen, das heißt Wechselwirkungen mit anderen Infrastrukturen,

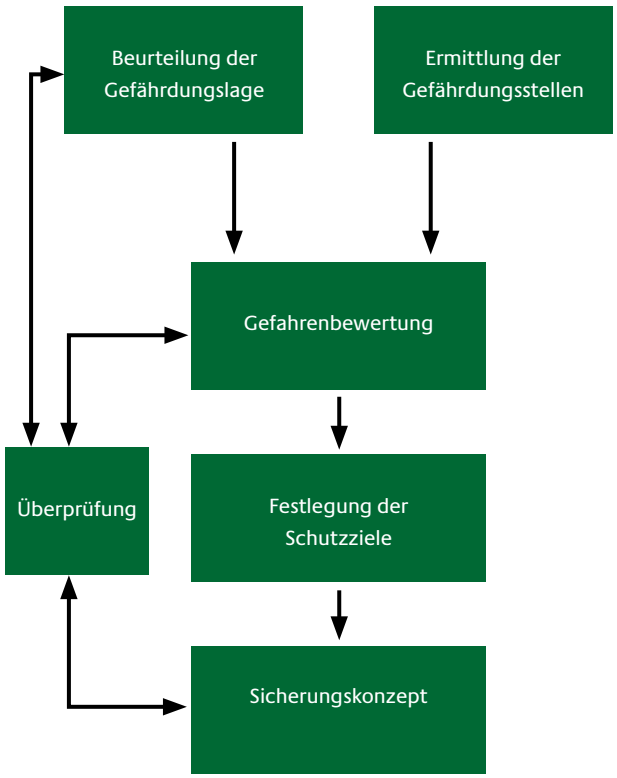
[3] modifiziert nach Störfallkommission, Maßnahmen gegen Eingriffe Unbefugter, 2002.

- Art, Topologie und Kooperationsbeziehungen der betreiberseitig vorhandenen Risikomanagementstrukturen,

- Strukturen der Zusammenarbeit zwischen öffentlichen Einrichtungen und Betreibern, sowohl mit Blick auf Notfallplanung und Krisenmanagement als auch unter Gesichtspunkten der technischen Prävention.

Bei der Analyse sind nicht nur Primärschäden aus Zwischenfällen zu berücksichtigen, sondern auch Sekundäreffekte (hierzu Seite 19).

Abbildung 2: Analyseschritte



Quelle: Störfallkommission, Maßnahmen gegen Eingriffe Unbefugter, 2002, S. 20

2 Gefährdungen und gefährdete Bereiche

2.1 Gefährdungen

Dominoeffekte/ Verzögerung/ Ablenkung

Die Gefährdungen, denen sich Betreiber von Kritischen Infrastrukturen gegenübersehen, lassen sich in (1) Gefährdungen durch natürliche Ereignisse, (2) Gefährdungen durch menschliches oder technisches Versagen und (3) Gefährdungen durch Terrorismus und kriminelle Handlungen einteilen. Dabei ist zu beachten, dass die Gesamtanlage oder sicherungsrelevante Teile der Anlage auch durch Ereignisse außerhalb der eigentlichen Anlage, in benachbarten Betriebsbereichen oder Verkehrsanlagen in Mitleidenschaft gezogen werden können, die einem besonderen Gefährdungspotenzial unterliegen (Dominoeffekt). Einwirkungsmöglichkeiten können zum Beispiel im Brandfall durch das Übergreifen eines Feuers von benachbarten Einrichtungen entstehen, durch den Flug von Trümmern nach einer Explosion in benachbarten Einrichtungen, durch den Ausfall von Versorgungseinrichtungen nach Katastrophen außerhalb der Anlage usw. Auch Ereignisse in engem zeitlichen Zusammenhang wie etwa eine zweite, verzögert einsetzende Explosion oder mehrere etwa zeitgleiche Störfälle an verschiedenen Orten, können unter Umständen eine exponentielle Wirkung hervorrufen, indem Rettungs- oder Wiederherstellungsmaßnahmen unterbunden oder Ressourcen an der falschen Stelle gebündelt werden (Ablenkungsmaßnahmen).

Abbildung 3: Risikofaktoren

Risikofaktoren

Die folgende Übersicht soll die Komplexität und Heterogenität der zu betrachtenden Risikofaktoren verdeutlichen, ohne dabei den Anspruch auf Vollständigkeit zu erheben:

Risikofaktor Mensch

- mangelndes Sicherheitsbewusstsein
- nicht hinreichend qualifiziertes Personal
- menschliches Versagen
- kriminelles Verhalten (Sabotage, Terroranschläge)

Risikofaktor Organisation

- Konzentration unverzichtbarer Ressourcen
- Outsourcing unternehmenskritischer Infrastrukturen

Risikofaktor Natur/Umwelt

- Naturkatastrophen
- Seuchen und Epidemien

Risikofaktor IT

- Komplexität der Systeme
- zunehmende IT-Abhängigkeit
- umfangreiche weltweite Vernetzung von IT-Systemen
- kurze Innovationszyklen der IT
- Standardisierung der Technik und Komponenten
- Vernetzung/Interdependenzen von Kritischen Infrastrukturen
- Internet als Nervensystem Kritischer Infrastrukturen (Zusammenhang mit IT-Security)

Quelle: Bundesverband deutscher Banken, Management von Kritischen Infrastrukturen, S. 13

2.1.1 Gefährdungen durch natürliche Ereignisse

Extremwetterlagen
In Deutschland resultieren nach Angaben der Versicherungswirtschaft die Elementarschäden zu einem großen Anteil aus atmosphärischen Extremereignissen. Hierzu zählen Ereignisse wie Hochwasser (inklusive Erhöhung des Grundwasserspiegels), Überschwemmungen, Überflutungen, Sturmfluten, Schnee, Eis, Dürren sowie Stürme. Besondere Gefahren bei Hochwasser entstehen durch die Kraft des Wassers bei der Unterspülung von Wegen, Brücken, Dämmen etc. und durch mitgeführtes Treibgut. Die Gefahr einer Trinkwasserverunreinigung und damit erheblicher gesundheitlicher Risiken wird durch ausgelaufene Schadstoffe und Unrat, die in den Fluten mitgeführt werden, noch erhöht. Durch steigenden Grundwasserspiegel können auch entfernter gelegene Gebiete überflutet werden.

Wirbelstürme und Hagel können Folge schwerer Gewitter sein und zusätzliche Gefahren hervorrufen. Als Stürme werden Luftbewegungen ab 75 km/h und als Orkan Luftbewegungen ab 120 km/h bezeichnet. Neben unmittelbaren Schäden, die durch Winddruck und nachfolgende Böen entstehen, können Stürme und Orkane zusätzliche Gefährdungen durch Trümmer und Schmutzteile, die durch den heftig rotierenden Schlauch eines Wirbelsturms mitgeführt werden, auslösen. Stürme nehmen sowohl bezüglich der Häufigkeit als auch der prozentualen Verteilung volkswirtschaftlicher Schäden eine Spitzenstellung ein.

Hagelkörner können in Einzelfällen eine Größe von mehr als 10 cm und ein Gewicht von über einem Kilogramm erreichen. Neben Sachschäden und Schäden an landwirtschaftlichen Kulturen können Hagelkörner auch erhebliche Verletzungen beim Menschen hervorrufen. Auch können Hagelkörner Wasserabflüsse verstopfen und so Überschwemmungen hervorrufen.

Erdbeben
Die Gefährdung durch Erdbeben wächst zwangsläufig mit steigender Intensität des Bebens. In Abhängigkeit von geologischen Parametern, wie zum Beispiel der Bodenbeschaffenheit, können jedoch auch schwächere Erdbeben umfangreiche Schäden an Gebäuden und Infrastrukturen hervorrufen. Zu berücksichtigen sind gegebenenfalls auch Sekundärschäden, wie zum Beispiel Brände und Flutwellen. Zu den erdbebengefährdeten Gebieten in Deutschland zählen insbesondere die Kölner Bucht, der Rheingraben und das Vogtland.

Flächenbrände
Flächenbrände können natürlicherweise durch Blitzschlag, Selbstentzündung oder durch vorsätzliche oder fahrlässige Brandstiftung in Kombination mit lang anhaltender Trockenheit entstehen. Hauptsächlich gefährdet sind Waldgebiete, landwirtschaftlich genutzte Flächen und Heideflächen.

Massenbewegungen
Massenbewegungen werden ausgelöst durch geophysikalische Ereignisse (zum Beispiel Erdbeben, Verwitterung), meteorologische Einflüsse (zum Beispiel Starkniederschläge, Überschwemmungen, Schnee- und Eisschmelze) und durch anthropogene Einflüsse (zum Beispiel Baumaßnahmen, Erschütterungen, Abholzungen). Beispiele für Massenbewegungen sind Lawinen, Muren, Hangrutschungen und Liquefaktion (Bodenverflüssigung).

Neben den direkten Schäden können Massenbewegungen auch indirekt Gefährdungen hervorrufen, indem Flutwellen in Seen oder Speichern erzeugt oder Flüsse abgeriegelt werden, die später aufbrechen.

Epidemien
Unter einer Epidemie wird das örtlich und zeitlich gehäufte Auftreten einer ansteckenden Krankheit bei Menschen oder Tieren verstanden. Eine erhöhte Gefährdung ergibt sich beispielsweise durch globalen Warenverkehr und Tourismus, durch Massentierhaltung sowie durch Überschwemmungen und Dürren. Bei einer Pandemie handelt es sich um eine länderübergreifende oder sogar weltweite Epidemie.

2.1.2 Gefährdungen durch menschliches und technisches Versagen

Brände
Ein Brand ist ein sich unkontrolliert ausbreitendes Feuer, das durch menschliches und technisches Versagen inklusive Brandstiftung (siehe unten, 2.1.3), durch Blitzschlag, durch die Freisetzung von Gefahrstoffen oder als Folge von Explosionen entsteht. Brände werden ihrer Größe entsprechend klassifiziert in Kleinbrände, Mittelbrände (zum Beispiel Gebäudebrände) und Großbrände (zum Beispiel Industriebetriebe, Großanlagen, Lager).

Freisetzung von Gefahrstoffen
Zu den Gefahrstoffen zählen alle Substanzen atomarer, biologischer, chemischer und radiologischer Art (ABCR/CBRN), die sich schädigend auf die Umwelt oder den Menschen auswirken beziehungsweise die zu Explosionen und Bränden führen können. Die Eigenschaften von Gefahrstoffen sind höchst unterschiedlich und reichen von reizend, leicht entzündlich bis zu explosionsgefährlich, umweltgefährdend, chronisch schädigend und toxisch. Mit Hilfe eines individuellen Gefahrstoffkatasters können die im Unternehmen genutzten Gefahrstoffe identifiziert werden.

Explosionen
Eine Explosion entsteht durch eine plötzliche Volumenausdehnung von Gasen durch die Freisetzung von Energie, die zu einer Druckwelle, gegebenenfalls mit einer Wärmeentwicklung führt. Explosionen können durch menschliches und technisches Versagen inklusive Vorsatz, durch Blitzschlag oder durch die Freisetzung von Gefahrstoffen entstehen.

Sonstige physische Einwirkungen von innen und von außen
Physische Einwirkungen von innen und von außen können durch Unfälle und Havarien wie zum Beispiel Verkehrs- oder Betriebsunfälle sowie Flugzeugabstürze (vgl. 2.1.3) hervorgerufen werden. Neben der Zerstörung der Anlage können Unfälle und Havarien auch zu Bränden und Explosionen, zur Freisetzung von Gefahrstoffen sowie zu anderen Schädigungen führen.

2.1.3 Gefährdungen durch Terrorismus und kriminelle Handlungen

Gefährdungsarten

Als Ergebnis der Analyse zur allgemeinen Gefährdungslage eines Unternehmens können Gefährdungen durch Terrorismus oder kriminelle Handlungen bestimmten abgestuften Gefährdungsarten zugeordnet werden. Die einzelnen Stufen geben dabei einen Überblick über eventuell zu erwartende Täter, deren mögliche oder auch typische Vorgehensweise, ihre Ziele und Motive sowie über den Grad der kriminellen Energie. Mit ihrer Hilfe kann übersichtlich dargestellt werden, welche Risiken in Betracht zu ziehen sind.

Die Annahmen innerhalb einer Gefährdungsart beruhen auf kriminalistischem Erfahrungswissen, müssen jedoch nicht in jedem Einzelfall genau zutreffen. Die Frage nach eventuell zu erwartenden Tätern und ihrer Handlungsweise ist naturgemäß nicht mit Sicherheit zu beantworten. Auf der Grundlage von Erfahrungen bei der Betriebssicherung lässt sich jedoch eine Grobeinteilung mit Verursacher- oder Tätergruppen, ihren typischen Motiven und möglichen Verhaltensweisen in einer nach Gefährlichkeit abgestuften Tabelle (siehe Seite 27) vornehmen. Fahrlässige Handlungen werden dabei nicht berücksichtigt, sie sind unter Gefährdungen durch Ereignisse menschlichen und technischen Versagens (Kapitel 2.1.2) mit erfasst.

Inwieweit potenzielle Täter tatsächlich ernsthaften Schaden anrichten können und an welcher Stelle dies möglich und wahrscheinlich ist, muss Gegenstand der Risikobewertung unter Berücksichtigung der im Umfeld des Unternehmens identifizierten Gefahrstellen sein (vgl. etwa den Abschnitt „Risikomanagement“ der Checkliste, Anhang 1). Die Gefährdungsarten enthalten eine Reihe von Annahmen, die eine Zuordnung zur ermittelten Gefährdungslage ermöglichen sollen. Zu diesen Annahmen gehören im Wesentlichen

- mögliche Begleitumstände der Tat,
- mögliche Motive und typische Handlungsweisen,
- wahrscheinlich verwendete Hilfsmittel und
- zu erwartende kriminelle Energie.

Des Weiteren lässt sich, im Sinne eines Bindegliedes zwischen Tätern respektive deren Motivationen und den Tatoptionen durch die Beschaffenheit der Infrastrukturen selbst, nach Einwirkungsmöglichkeiten differenzieren. Prinzipiell denkbare Einwirkungsmöglichkeiten sind beispielsweise folgende:

Einwirkungsmöglichkeiten

Vorsätzliches Fehlbedienen
Hierunter sollen alle vorsätzlichen Handlungen verstanden werden, bei denen durch einfache Handgriffe und ohne Einsatz von Tatmitteln eine Störung ausgelöst werden könnte. Zu derartigen Handlungen könnten zum Beispiel zählen: das Schalten und Abschalten von Einrichtungen, Auf- und Zudrehen von Rohrleitungsverschlüssen (Schiebern), Drehen von Handrädern und das Betätigen von Hebeln im Prozessverlauf. Das vorsätzliche Fehlbedienen kann dabei sowohl durch eigenes Personal als auch durch Betriebsfremde vorgenommen werden.

Manipulieren
Unter Manipulieren wird das vorsätzliche Verändern oder Verstellen von Systemteilen zum Zwecke des Herbeiführens eines kritischen Anlagenzustandes verstanden. Beispiele hierfür könnten sein: das Fehlprogrammieren von Steuerungen, Dejustieren von Messeinrichtungen, Unterdrücken von Prozess-, Stör- oder Alarmmeldungen oder auch das Ausschalten von Schutzsystemen. Als Täter kommen vorrangig „Insider“ mit genauen Anlagenkenntnissen in Frage.

Fahrzeugunfall
Durch bewusst herbeigeführte Fahrzeugunfälle im Straßen- oder Schienenverkehr des Betriebsbereichs könnten gefährliche Stoffe freigesetzt oder wichtige Anlagenteile beschädigt beziehungsweise zerstört werden. Beispiele hierfür sind Fassleckage durch Gabelstaplerunfall, Entgleisen von Kesselwagen, Zerstören von Anlagen durch LKW-Aufprall.

Eingriffe mit einfachen Tatmitteln
Hier ist an ein vorsätzliches, oft spontanes Eingreifen in wichtige Anlagenteile mit den in jedem Betrieb vorhandenen Hilfsmitteln und Werkzeugen gedacht. Beispiele könnten sein: das Zerschlagen von Glasteilen der Anlage, Festklemmen beweglicher Teile der Anlage oder auch das Zumischen nicht erlaubter Stoffe in den Prozess. Als mögliche Täter kommen dabei in erster Linie Beschäftigte des Unternehmens in Betracht.

Eingriffe mit schweren Tatmitteln
Bei dieser Einwirkungsmöglichkeit wird das vorbereitete gewaltsame Zerstören von Anlagenteilen unterstellt. Als Angriffswerkzeuge können zum Beispiel Brechstangen, elektrische Bohrmaschinen, Schneidbrenner, Bolzenschneider oder Vorschlaghammer in Frage kommen. Beispiele hierfür sind das Aufbrechen von Türen und anschließendes Zerstören von Einrichtungen, Zerschlagen von Mess- und Steuereinrichtungen und das Aufschlagen von Behältern und Rohrleitungen mit der Folge größerer Leckagen. Anstelle des gezielten Anschlages kann auch Vandalismus treten, so zum Beispiel als blinde Zerstörungswut nach einem erfolglosen Einbruch.

Brandstiftung mit einfachen Mitteln
Unter einfachen Mitteln wird das Zünden mit Streichhölzern, Feuerzeugen oder durch Zigarettenkippen verstanden. Die Einwirkungsmöglichkeit besteht daher nur beim Vorhandensein ausreichender Mengen brennbaren, leicht entzündlichen Materials. Beispiele könnten sein: das Anzünden von brennbaren Flüssigkeiten aus dem verfahrenstechnischen Ablauf, Inbrandsetzen von Lagerstellen mit der Folge des Freisetzens gefährlicher Stoffe, Inbrandsetzen von peripheren Räumen oder Einrichtungen mit Auswirkungen auf wichtige Anlagenteile.

Brandstiftung mit brandfördernden Mitteln
Hier geht es um Brandanschläge, die mit Hilfe von schnell und intensiv abbrennenden Stoffen ausgeführt werden. Beispiele für Anschläge können sein: das Ausgießen und Anzünden von brennbaren Flüssigkeiten (zum Beispiel Benzin), Werfen von so genannten „Molotow-Cocktails“ (zum Beispiel auch durch Fenster) oder auch das Anbringen professioneller Brandsätze mit Zeit- oder Fernzündeinrichtungen. Die Anschläge können auch von außen durchgeführt werden (Wurfentfernung) und setzen eine ausgeprägte kriminelle Energie voraus.

Einsatz von Sprengstoffen
Hier könnten Selbstlaborate, gewerbliche oder militärische Sprengstoffe eingesetzt werden. Mögliche Angriffsbeispiele sind beispielsweise das Anordnen einer „Feuerlöscher-Bombe“ als Selbstlaborat innerhalb empfindlicher Anlagenteile oder wahrscheinlicher an der Gebäudeperipherie, Aufsprengen von Behältern und Rohrleitungen, Wegsprengen von tragenden Bauteilen mit der Folge des Umstürzens von Behältern, Zerstören von Anlagenteilen. In der Regel liegt bei dieser Angriffsart Fremdeinwirkung mit radikal-politischem Hintergrund vor.

Beschuss
Im einfachsten Fall ist mit dem Beschuss durch Luftdruckgewehre oder Schleudern (Stahlkugel) zu rechnen bis hin zum Einsatz schwerer Waffen – beispielsweise Flugabwehrraketen – durch terroristische Täter. Beispiele für Einwirkungsmöglichkeiten: Verursachen von Leckagen in freistehenden Behältern oder in Rohrleitungen, Herbeiführen einer Explosion. Ein Beschuss ist vor allem von außerhalb der äußeren Umfriedung eines Betriebsbereichs beziehungsweise Industrieparks möglich, wobei in Zaunnähe installierte Anlagenteile stärker gefährdet sind.

Flugzeugabsturz
Hier können sowohl die kinetische Energie abstürzender Maschinen als auch die Explosionswirkung des mitgeführten Treibstoffes oder an Bord befindlichen Sprengstoffs zum Tragen kommen. Des Weiteren kann ein Flugzeug als Transportmedium für die Ausbreitung von ABCR-Substanzen genutzt werden. Angriffe, die zum Absturz führen, können von außen, zum Beispiel durch Raketenbeschuss, Fernzündung von Sprengstoff, Fernmanipulation an der Bordelektronik, Ausfall oder Missbrauch der Flugsicherungsleitstellen, oder von innen mittels Übernahme oder Störung der Steuerung oder durch Zündung von Sprengstoff (Selbstmordattentäter) herbeigeführt werden.

Einsatz von ABCR-Waffen
In Abhängigkeit von der Verfügbarkeit entsprechender Agenzien/Tatmittel ist ein breites Spektrum von Einsatzmöglichkeiten denkbar, das gesonderter Erörterung bedarf. Die Einsatzmöglichkeiten reichen vom vorsätzlichen Auslösen von Erkrankungen (Versand von Milzbranderregern) beziehungsweise Epidemien (Einbringen von hochinfektiösen Erregern in Versorgungssysteme oder über die Atemluft) über den Einsatz so genannter „dirty bombs“ mit dem Ziel der nachhaltigen Verunsicherung der Bevölkerung bis hin zum Giftgaseinsatz beispielsweise an Verkehrsknotenpunkten.

Kombinationswirkungen
Auch hier ist ein breites Spektrum an Möglichkeiten denkbar: von den bereits erwähnten dirty bombs als Kombination aus Explosivwirkung und radioaktiver Kontamination über die Zerstörung einer Produktionsanlage plus Ausbreitung von Schadstoffen bis hin zur medienwirksamen Einzelaktion mit weit reichenden Folgen für Unternehmensaktivitäten oder die Versorgung der Bevölkerung.

2.2 Gefährdete Bereiche in Unternehmen

Kritische Infrastrukturen, aber auch einzelne Produktions- oder Dienstleistungsbereiche innerhalb einer Anlage sind in unterschiedlichem Maß von Gefährdungen durch natürliche Ereignisse, durch menschliches oder technisches Versagen sowie durch Terrorismus oder kriminelle Handlungen betroffen. Aus Unternehmenssicht können sich zusätzliche Gefährdungen beispielsweise durch Personalabbau, Zentralisierung und Automatisierung von Regelungs- und Überwachungsprozessen, Verlagerung von Zuständigkeiten infolge Outsourcings oder Vollzugsdefizite infolge Kostendrucks ergeben.

2.2.1 Durch natürliche Ereignisse besonders gefährdete Bereiche

Durch Extremwetterlagen besonders gefährdete Bereiche
Sturm- und Sturzfluten können die Zerstörung ganzer Gebäude und Anlagen hervorrufen. Zu den besonders gefährdeten Bereichen gehören neben den Netzen insbesondere auch Gebäude, Produktions-, Gewinnungs- und Verarbeitungsanlagen sowie nicht elektronische Datenbestände. Langsam abfließende Hochwasser führen hauptsächlich zu Schäden in tiefer gelegenen Gebäudebereichen (Untergeschoss, Erdgeschoss). Da Schäden durch Wassereinwirkung in der Regel Netzausfälle verursachen, sind die Informations- und Kommunikationstechnik, die (betriebsinterne) Stromversorgung sowie Versorgungs- und sonstige Leitungsnetze besonders gefährdet. Außerhalb der Überschwemmungsgebiete können diese Schäden durch steigenden Grundwasserspiegel hervorgerufen werden.

Unabhängig von ihrer Lage sind grundsätzlich alle Gebäude und Anlagen Stürmen ausgesetzt, besonders gefährdet sind aber Gebäude und Anlagen an exponierter Stelle (Berge, Hügel, Bergkämme, Windschneisen) sowie Gebäude und Anlagen, die dem Sturm Angriffsflächen bieten.

Stürme, aber auch Dürren oder extremer Frost können zudem zu Versorgungsengpässen führen, die einen geregelten Betriebsablauf nicht mehr gewährleisten.

Durch Erdbeben besonders gefährdete Bereiche
Durch Erdbeben können Gebäude und ganze Anlagenkomplexe geschädigt oder zerstört werden und Ausfälle in allen Bereichen hervorgerufen werden. Es ist nicht auszuschließen, dass auch leichte Erdstöße Schäden im Bereich IT und in erschütterungssensiblen Bereichen von Produktion, Gewinnung und Verarbeitung verursachen können.

Durch Flächenbrände besonders gefährdete Bereiche
Flächenbrände können alle Bereiche schädigen, soweit sich Gebäude oder Anlagen in diesem Bereich befinden. Zudem können Flächenbrände dazu führen, dass ganze Gebiete oder auch Verkehrswege gesperrt werden, wodurch Anlagen nicht oder nur schwer zu erreichen sind.

Durch Massenbewegungen besonders gefährdete Bereiche
Massenbewegungen können Gebäude und Anlagen insgesamt schädigen oder zerstören oder den Zugang zu diesen Anlagen und Gebäuden versperren. Doch auch Massenbewegungen außerhalb einer Anlage mit Auswirkungen auf externe Netze können zu Versorgungsengpässen führen, die einen geregelten Betriebsablauf nicht mehr gewährleisten.

Durch Epidemien besonders gefährdete Bereiche
Epidemien können zum Ausfall oder zu Engpässen des für den Betrieb der Anlagen notwendigen Fachpersonals führen. Hiervon wären insbesondere der Produktionsbetrieb sowie die Bereiche Rechenzentrum und Leitstellen betroffen. Zudem kann durch die Absperrung von Gebieten während Epidemien und Tierseuchen die Erreichbarkeit von Anlagen beeinträchtigt oder nicht möglich sein.

2.2.2 Durch menschliches und technisches Versagen besonders gefährdete Bereiche

Durch Brände besonders gefährdete Bereiche
Brände können von innen und von außen auf Anlagen und Gebäude einwirken. Sie können alle Bereiche zerstören, schädigen oder – etwa durch Brandraucheinwirkung – eine weitere Nutzung unterbinden. Auch kleine Brände in exponierten Anlagenteilen (zum Beispiel IT) können zum Ausfall der gesamten Anlage führen.

Durch Gefahrstoffe besonders gefährdete Bereiche
Bei der Freisetzung von Gefahrenstoffen kann es neben Schädigungen des Betriebspersonals und der Umgebung der Anlage als Hauptgefährdungen auch zu den Auswirkungen von Explosionen und Bränden kommen. Kontaminierte technische Anlagen einschließlich der IT-Geräte sind teilweise nicht oder nur in beschränktem Maße weiterverwendbar.

Durch Explosionen besonders gefährdete Bereiche
Explosionen können von innen und von außen auf Anlagen und Gebäude einwirken. Sie können alle Bereiche schädigen oder zerstören und Kettenreaktionen nach sich ziehen. Die Hauptzerstörung wird durch die Druckwelle verursacht; in der Folge der Explosion kommt es häufig zu Bränden. Bereits kleine Explosionen in sensiblen Bereichen (IT, Strom) können zum Ausfall der gesamten Anlage führen.

Durch sonstige physische Einwirkungen von innen und von außen besonders gefährdete Bereiche
Physische Einwirkungen von innen und von außen können die Funktionsfähigkeit der Anlage beeinträchtigen oder Gebäude und ganze Anlagenkomplexe schädigen oder zerstören. Dies kann Ausfälle in allen Bereichen hervorrufen. Physische Einwirkungen im Bereich der externen Netze können zu internen Versorgungsengpässen und Produktionsausfällen führen.

2.2.3 Durch Terrorismus und kriminelle Handlungen besonders gefährdete Bereiche

Die abgestuften Gefährdungsarten mit ihren Hinweisen auf prinzipiell denkbare Bedrohungen betreffen zunächst das gesamte Unternehmen. Doch selbst innerhalb des Gesamtunternehmens setzen sich einzelne Unternehmenskomplexe wiederum aus Bereichen, Einheiten oder Anlagenteilen zusammen, die sich nach Gefahrenpotenzial, Bauart, Nutzung, technischer Auslegung und vor allem in ihrer Verletzbarkeit gegenüber Störungen unterscheiden.

Auch innerhalb von Anlagenteilen sind in der Regel Stellen besonderer Verletzlichkeit vorhanden. Diese sind anhand einer getrennten Untersuchung systematisch zu ermitteln. In Analogie zu dem nach § 9 Störfallverordnung (StörfallV) zu erstellenden Sicherheitsbericht sind auch im Falle der Objektsicherung sowohl die eigentlichen Gefährdungspotenziale als auch die Einrichtungen zur Versorgung und Steuerung der Anlagen sowie die Stofftransportsysteme usw. von Bedeutung.

Klassifizierung von Sicherheitsbereichen

In der Regel ist es deshalb sinnvoll, den Betriebsbereich in eine Anzahl von Teilbereichen unterschiedlicher Art und Gefährdung aufzuteilen. Eine vollständige Analyse aller potenziellen Schwachpunkte, kombiniert mit den vielfältigen, denkbaren Einwirkungsmöglichkeiten ergäbe eine nicht beherrschbare Zahl von Varianten. Von daher erscheint eine stärker generalisierende Zusammenfassung von Anlagebereichen oder -teilen sinnvoll. So kann es zum Beispiel sinnvoll sein, einen zusammenhängenden Komplex als Ganzes zu betrachten, also ohne nähere Untersuchung, welche einzelnen Komponenten und Teile anfällig sind und welche genaue Auswirkung ein eventueller Angriff auf die eine oder andere Komponente der Anlage zur Folge hat. Der betreffende Anlagenkomplex wird als sicherungsrelevant eingestuft und insgesamt so gesichert, dass alle Einzelkomponenten mit erfasst sind.

Bei Versorgungssystemen, die im gesamten Betriebsbereich eingesetzt sind, sollten möglichst Teilbereiche bezüglich bedrohter Objekte gebildet und die Untersuchung nicht unnötig auf umfangreiche Gesamtnetze ausgeweitet werden. Gleichwohl bedeutsam bleibt der Blick über die eigenen Betriebs-

grenzen hinaus, sowohl hinsichtlich besonderer Gefährdungen im Bereich der vor- und nachgelagerten Wertschöpfungskette als auch bezüglich räumlicher Wechselwirkungen mit benachbarten Gefahrenstellen.

Bildung von Teilbereichen

Sinnvolle Zusammenfassungen von Gefährdungsbereichen können zum Beispiel sein:

- Produktions-, Gewinnungs- und Verarbeitungsanlagen,
- Leitzentralen, IT-Anlagen,
- (unbemannte) Außenanlagen,
- Versorgungsleitungen,
- Energieversorgungsanlagen aller Art,
- Notaggregate aller Art.

3 Generalisierende Basisschutzempfehlungen

Basisschutz als Mindestschutz

Ziel ist es, Basisschutzempfehlungen für unterschiedliche Gefährdungen vorzulegen, die als Mindestschutz stationärer Anlagen im Bereich der Kritischen Infrastrukturen anzusehen sind. Hierfür bietet sich ein mehrstufiges Verfahren in Anlehnung an das unter Kapitel 1 (Zielsetzung und methodische Grundlagen, S. 8) beschriebene Verfahren an, das eine Ermittlung der Risiken sowie die Entwicklung und die Umsetzung verschiedener Schutzmaßnahmen umfasst.

3.1 Analyse des Schutzbedarfs

3.1.1 Verfahren zur Analyse des Schutzbedarfs

Risikoabschätzung

Zunächst ist eine Prüfung der Standorte der KRITIS-Einrichtungen vorzunehmen. Hierzu gehört eine Risikoabschätzung bezogen auf natürliche Ereignisse, auf Ereignisse durch technisches und menschliches Versagen sowie auf terroristische Angriffe und kriminelle Handlungen. Risikoabschätzungen bezüglich der Gefährdungen durch natürliche Ereignisse können anhand von Plänen (Überflutungspläne, Erdbebenkarten, Raumordnungspläne, Risikokarten) durchgeführt werden, die bei den zuständigen Behörden (vgl. Kapitel 4) angefordert werden können. Bezüglich der Gefährdungen durch menschliches und technisches Versagen ist die Beachtung einschlägiger Vorschriften und technischer Regelwerke (zum Beispiel Brandschutz, Gefahrstoffverordnung, Arbeitsschutz, Schulungen) zu überprüfen. Mit Blick auf terroristische Gefährdungen können die Betreiber Kritischer Infrastrukturen

- in Zusammenarbeit mit den für die Innere Sicherheit zuständigen Behörden (vgl. Kapitel 4) kritische Unternehmensbereiche und Anlagen systematisch daraufhin untersuchen, ob sie prinzipiell ein herausgehobenes Ziel darstellen können und damit die Möglichkeit einer Beeinträchtigung oder (Zer-)Störung der Einrichtung besteht (Gefährdungsanalyse),
- in Zusammenarbeit mit den für die außerbetriebliche Gefahrenabwehr zuständigen Behörden (vgl. Kapitel 4) untersuchen, welche konkreten Auswirkungen aufgrund einer möglichen Beeinträchtigung oder (Zer-)Störung der Einrichtung zu erwarten sind und ob diese zu einer ernsten Gefahr führen könnten (Gefahrenanalyse),
- Unterschiede und Gemeinsamkeiten zwischen den Erfordernissen des Schutzes gegen Eingriffe Unbefugter, vor Naturgefahren und vor menschlichem wie technischem Versagen herausarbeiten.

Verständigung über Schutzniveau

Gefährdungsanalyse und Gefahrenanalyse sind gleichwertige Elemente der Analyse des Schutzbedarfs. Mit welchem dieser Schritte begonnen wird, sollte im Einzelfall entschieden werden. Im Rahmen dieses Konzepts wird vorgeschlagen, zunächst eine allgemeine Gefährdungsanalyse durchzuführen und die konkreten Auswirkungen dieser Gefährdungen auf das Unternehmen durch eine Gefahrenanalyse zu ermitteln, um sich auf dieser Basis über das Schutzniveau zu verständigen und dieses festzulegen. Die Analyse und die daraus abgeleiteten Maßnahmen sollten dokumentiert werden (vgl. Kapitel 3.5.2).

Diese Dokumentation ist jedoch in besonderem Maße geheimhaltungsbedürftig und sollte auch innerhalb des Unternehmens nur einem beschränkten Kreis von Beschäftigten zugänglich sein. Aus Unterlagen, die dem Personal insgesamt und der Öffentlichkeit zur Verfügung stehen, sollte jedoch

schlüssig hervorgehen, dass der Betreiber die notwendigen Maßnahmen zur Sicherung des Unternehmensbereichs und der Anlagen getroffen hat (vgl. Kapitel 3.3.1). Darüber hinaus ist die Analyse in regelmäßigen Zeitabständen zu wiederholen und in den Risikomanagementprozess des Unternehmens zu integrieren, um neue Gefährdungen erkennen und eine erforderliche Neubewertung vornehmen zu können, den Schutzbedarf entsprechend anzupassen und damit die Aktualität des Basisschutzes sicherzustellen.

3.1.2 Berücksichtigung von Abhängigkeiten und Wechselwirkungen

Neben unmittelbaren Gefährdungen durch natürliche Ereignisse, durch menschliches und technisches Versagen oder durch Terrorismus und kriminelle Handlungen sind Kritische Infrastrukturen auch mittelbar Gefährdungen ausgesetzt, die bei der umfänglichen Analyse des Schutzbedarfes zu berücksichtigen sind.

Dominoeffekte

Hier sind zum einen die so genannten Dominoeffekte zu bestimmen, die entstehen, wenn sich externe Ereignisse, zum Beispiel in benachbarten Betriebsbereichen, in der Umgebung oder im Verkehrsbereich, auf die Anlage auswirken. So können sich weiter entfernte Naturereignisse wie Hochwasser, Massenbewegungen oder Erdbeben mittelbar durch Rückstau, Verschüttung von Zufahrts- und Lieferwegen auf die Funktionsfähigkeit der Anlage auswirken. Störungen in umgebenden Anlagen, insbesondere mit besonderem Gefährdungsrisiko, können die Anlage durch Übergreifen eines Feuers oder Trümmerflug nach einer Explosion schädigen. Auch ist der Ausfall von Versorgungseinrichtungen wie Energie- und Wasserversorgung oder von Dienstleistungen durch Zulieferer aufgrund von Katastrophenereignissen außerhalb der Anlage möglich.

Ereignisse in engem zeitlichen Zusammenhang wie mehrere etwa zeitgleiche Störfälle an verschiedenen Orten oder auch eine zweite, verzögert einsetzende Explosion können unter Umständen eine exponentielle Wirkung hervorrufen, indem beispielsweise Rettungs- oder Wiederherstellungsmaßnahmen unterbunden oder Ressourcen an der falschen Stelle gebündelt werden (Ablenkungsmaßnahme).

Sekundärschäden

Daneben können durch die Beeinträchtigungen von Kritischen Infrastrukturen zusätzliche Schäden hervorgerufen werden (Sekundärschäden), etwa die mit Störungen im Transportwesen nach einem Stromausfall verbundenen Versorgungs- oder Lieferengpässe. Auch diese Sekundärschäden sind bei der Analyse des Schutzbedarfes zu berücksichtigen, um die Folgen eines vollständigen oder auch nur bereichsspezifischen Ausfalls Kritischer Infrastrukturen auf Bereiche innerhalb der Anlage, aber auch außerhalb angemessen bewerten zu können.

3.1.3 Besondere Berücksichtigung von Terrorismus und kriminellen Handlungen

Bereits erstellte Gefährdungs- und Gefahrenanalysen sowie Sicherheitskonzepte sollten darauf überprüft werden, ob auch diejenigen Gefahren berücksichtigt sind, die gemäß Gefährdungsanalyse durch Eingriffe Unbefugter ausgelöst werden können, selbst wenn sie als Störungen, natürliche Risiken oder Unfälle weitgehend ausgeschlossen wurden.

Falls in der Gefahrenanalyse festgestellt wurde, dass für besondere Schutzobjekte eine ernste Gefahr bestehen kann, ist zu prüfen, inwieweit die Anlagen für terroristische Angriffe und kriminelle Handlungen besonders „attraktiv“ erscheinen. Dazu ist eine systematische Analyse durchzuführen, in der insbesondere die folgenden, bereits unter Kapitel 1 (Zielsetzung und methodische Grundagen, S. 8f.) aufgeführten Aspekte zu berücksichtigen sind:

Inhalt Analyse- und Planungsprozess

- Beurteilung der Gefährdungslage,
- örtliche Lage des Betriebsbereichs und der Anlagen,
- Bedeutung der Anlagen für vor- und nachgelagerte Produktionsprozesse und Dienstleistungen,
- Symbolcharakter des Unternehmens beziehungsweise der Anlagen,

- Interdependenzen, das heißt Wechselwirkungen mit anderen Infrastrukturen,
- Art, Topologie und Kooperationsbeziehungen der betreiberseitig vorhandenen Risikomanagementstrukturen,
- Strukturen der Zusammenarbeit zwischen öffentlichen Einrichtungen und Betreibern.

Zusammenarbeit mit Sicherheitsbehörden

Die hierfür erforderlichen Informationen müssen die Betreiber zum Teil bei den für die Innere Sicherheit zuständigen Behörden (vgl. Kapitel 4) einholen, deren Einbindung in diesem Schritt ohnehin zu empfehlen ist.

Die allgemeine Sicherheitslage beschreibt Gefährdungen, wie sie für Betriebsbereiche generell gelten, gegebenenfalls mit regionalen Unterschieden. Gradmesser hinsichtlich relevanter Kriminalität sind in einem ersten Schritt die polizeiliche Kriminalstatistik sowie Veröffentlichungen der Versicherer. Die Sicherheitslage hinsichtlich politisch motivierter Straftaten wird bestimmt durch laufende Erkenntnisse der Behörden aufgrund ihrer kriminalpolizeilichen und verfassungsschutzmäßigen Tätigkeiten. Hiernach können auch regionale Aspekte stärker berücksichtigt werden.

Umfang, Schwere und Art der in einem Betriebsbereich bisher festgestellten Delikte können Hinweise auf den Gefährdungsgrad geben. Dabei kann ein Zeitraum von etwa fünf Jahren angesetzt werden. Insgesamt sollten die folgenden Informationen enthalten sein:

- pauschale Angaben über festgestellte kleinere Delikte wie zum Beispiel einfacher Diebstahl,
- Anzahl der bisher verübten Einbrüche oder schweren Diebstahlsdelikte,
- Feststellung von organisierter Kriminalität im Betriebsbereich,
- Anzahl bisher verübter Sabotagehandlungen einschließlich unaufgeklärter Fälle, bei denen ein erheblicher Sabotageverdacht besteht,
- Anzahl bisheriger Bombendrohungen oder anderweitiger Bedrohungshandlungen,
- Anzahl bisheriger Brandstiftungen oder Sprengstoffanschläge inklusive der Verdachtsfälle.

3.2 Festlegung von Schutzzielen

Um Schutzziele definieren und operationalisieren zu können und sie auch in der Unternehmenspolitik dauerhaft zu verankern, empfiehlt sich ihre Festlegung im Rahmen eines Sicherheitsmanagementsystems. Managementsysteme haben sich in der Vergangenheit als Instrument zur systematischen Handhabung und Überprüfung von Unternehmensabläufen bewährt, sofern sie eine gelungene Synthese zwischen Top-down-Ansätzen (hierarchisch, zentral), Bottom-up (diskursiv, dezentral) und Querdenken (innovativ, vernetzt) gewährleisten konnten. Vor allem im Zusammenhang mit Unternehmenssicherheit ist eine systematische Integration verschiedener sicherheitsrelevanter Prozesse, sowohl untereinander als auch mit den Wertschöpfungsstrategien, von größter Bedeutung. Viele dieser Maßnahmen werden bereits praktiziert oder können vergleichsweise rasch eingeführt werden. Die Betreiber sollten die Wirksamkeit bestehender Maßnahmen, soweit noch nicht geschehen, überprüfen und gegebenenfalls reagieren (vgl. auch Kapitel 3.5.1).

Dabei kommt der qualitativen und quantitativen personellen und technischen Ausstattung des internen oder externen Sicherheitsdienstes (zum Beispiel Werkschutz) besondere Bedeutung zu; Anforderungen ergeben sich unter anderem aus der DIN 77200. Des Weiteren ist auf die Vernetzung und Harmonisierung oft weitgehend eigenständiger Teile des Sicherheitsmanagements, wie IT-Sicherheit, Objektschutz und Personalsicherheit, besonderer Wert zu legen. Gehört der zu untersuchende Betriebsbereich zu einem größeren Unternehmen (Unternehmensbereich, Tochter, Mehrheitsbeteiligung etc.), so müssen Gefährdungs- und Gefahrenlage des Gesamtunternehmens zusätzlich berücksichtigt werden. Dies gilt vor allem auch in Hinblick auf politisch motivierte Straftaten. Erfahrungsgemäß wächst diese Gefahr allgemein mit der Größe und (globalen) Bedeutung des Gesamtunternehmens.

In diesem Zusammenhang sollte auch festgestellt werden, ob durch bestimmte Vertriebsverbindungen höhere Risiken bestehen. Dies könnte zum Beispiel der Fall sein bei Geschäftsverbindungen mit

politisch instabilen Ländern. Da Betriebsbereiche mit Exportausrichtung in der Regel meist in alle Welt liefern, besteht ein erhöhtes Risiko vor allem bei besonders herausragenden Verbindungen zu derartigen Ländern.

Kernschutzziele

Wesentliche Schutzziele für die Sicherung von Anlagen und Objekten, die als sicherungsrelevant eingeschätzt werden, können wie folgt beschrieben werden:

- Die Grenzen von Betriebsbereichen sind durch technische und organisatorische Maßnahmen so zu sichern, dass Unbefugte ohne Anwendung von Gewalt oder arglistige Täuschung nicht eindringen können und ein gewaltsames Eindringen in angemessener Zeit erkannt wird.
- Betriebsfremde sollten identifizierbar sein.
- Die Anlagen selbst sind so zu sichern, dass unbefugte Eingriffe ohne interne Kenntnisse und/oder technische Hilfsmittel nicht vorgenommen werden können.
- Finanzielle Ressourcen sollten gemäß Prioritätenlisten eingesetzt werden (integratives Sicherungsmanagement).
- Industrieparks stellen allein wegen der Vielzahl rechtlich und organisatorisch selbstständiger Betreiber besondere Anforderungen an die Sicherungsmaßnahmen. Die Angreifbarkeit gefährlicher Anlagen kann hier in der Regel nur durch gemeinsam abgestimmte Schutzziele und Maßnahmen minimiert werden. Die Auswahl geeigneter Maßnahmen erfolgt zweckmäßigerweise gemäß einer systematischen Sicherungsanalyse.

3.3 Maßnahmen zur Erreichung der Schutzziele

Maßnahmen gegen Eingriffe Unbefugter

Zum Schutz von Anlagen und Objekten, die als sicherungsrelevant eingeschätzt werden, sollten Ziele festgelegt werden. Bereits seit vielen Jahren sind Betreiber von Anlagen, die der Störfallverordnung unterliegen, verpflichtet, ihre Betriebsbereiche und Anlagen gegen Eingriffe Unbefugter zu sichern. Angesichts spezifischer Bedrohungssituationen (Terrorismus) ist ein Eindringen von Unbefugten auch in nicht der Störfallverordnung unterliegende Betriebsanlagen Kritischer Infrastrukturen zu erschweren. Dazu gehören wirkungsvolle Maßnahmen wie etwa überwachte Umzäunungen, Organisation von Torkon-trollen, Streifengänge, Videoüberwachung etc. (vgl. auch Checkliste, Anhang 1).

Eine Gefährdung von Betriebsbereichen und Anlagen durch terroristische Angriffe ist sowohl hinsichtlich der Wahrscheinlichkeit als auch der potenziellen Folgen differenziert zu betrachten. Bisher schon gebräuchliche Sicherungsmaßnahmen bieten nach wie vor erheblichen Schutz. Sie sollten daher konsequent und unter Berücksichtigung der in diesem Konzept gemachten Empfehlungen angewendet werden, so weit dies nach dem 11.9.2001 erforderlich erscheint und noch nicht geschehen ist. Besonders gefährliche und hinsichtlich terroristischer Anschläge gefährdete Anlagen oder Anlagenteile sind zusätzlich zu sichern.

Um die definierten Schutzziele zu erreichen, sind entsprechende Maßnahmen zu ergreifen. Diese lassen sich in innere und äußere Schutzmaßnahmen (physischer Schutz), in personelle Schutzmaßnahmen sowie in organisatorische Schutzmaßnahmen und Maßnahmen des Managements unterteilen.

3.3.1 Innerer und äußerer Schutz

Zu den Maßnahmen zur Erreichung der Sicherungsziele für den inneren und äußeren Schutz der Anlagen gehören beispielsweise die folgenden:

- Besonders sensible Bereiche sollten nicht in hochwasser- und erdbebengefährdeten Bereichen gebaut werden. Liegen sie bereits in diesen Gebieten, sollte eine Verlegung in nicht gefährdete Gebiete in Betracht gezogen werden; zumindest sollten spezielle Sicherungsmaßnahmen gegen Überschwemmungen und Erdbeben getroffen werden (zum Beispiel Hochlegung der IT und Stromverteiler, Abfederung gegen Erschütterungen, Eindeichen).
- Eine Härtung von gesamten Anlagen oder von besonders sensiblen Anlagenteilen sollte vorgenommen werden, um Auswirkungen von Sturm- und Sturzfluten sowie von Erdbeben, von physischen

Härtung und Zugangssicherung

Einwirkungen und von Explosionen zu vermindern oder zu vermeiden. Es sind ausreichende Widerstandsreserven in den unteren Geschossen einzuplanen (Druckausgleich). Zudem sollten besonders sensible Bereiche im Inneren der Anlagen liegen.

- Eine wesentliche Komponente der Prävention terroristischer Anschläge oder Sabotage ist die Erzeugung von räumlicher und zeitlicher Distanz zum schützenswerten Objekt. Barrieren und Hindernisse können einen Zugang zu sensiblen Bereichen be- oder verhindern (Zugangszonen, Zugangskontrollen, Werkschutz, Pforte, Umzäunungen, Streifengänge, Poller, Betonelemente, Höhensprünge).
- Nicht einsehbare Bereiche können durch elektronische Sicherungssysteme kontrolliert werden (Videoüberwachung, Bewegungsmelder, Geräuschmelder, Wärmebildkameras, Nachtsichtgeräte).
- Den Pforten kommt über die Aufgabe der Zufahrts- und Zugangskontrolle hinaus meist zusätzliche Sicherungsbedeutung zu. In diesem Zusammenhang stellt sich deshalb die Frage nach der Sicherung der Pforte selbst. Ist zum Beispiel die Hauptpforte die einzige Stelle für das Entgegennehmen von Alarm- und Störmeldungen (häufig auch erst nach der normalen Dienstzeit des Betriebsbereichs), so darf die Weitergabe der Meldungen an hilfeleistende Stellen nicht durch Zugriff auf die Fernmeldeeinrichtungen oder Bedrohungen des Werkschutzes an der Pforte unterbunden werden können. Dies ist durch geeignete Schutzmaßnahmen sicherzustellen. Auch ist die ständige Besetzung der Pforte beziehungsweise der Sicherungszentrale von zentraler Bedeutung.
- Das Personal ist im Hinblick auf die Sicherung des Betriebsbereichs zu sensibilisieren und einzubeziehen, durch Teamtraining, Seminare, Schulungen etc.

Grundschutz – Spezialschutz

In den meisten Fällen haben die Maßnahmen zur Sicherung des Gesamtgeländes die Funktion eines Grundschutzes; sie bilden eine erste Schwelle zur Abwehr unbefugter Personen. Der individuelle Spezialschutz aller vorhandenen Gefährdungsstellen muss zusätzlich erbracht werden. „Klassische" Maßnahmen zur Anlagen- und Objektsicherheit spielen hierbei eine wesentliche Rolle.

Die Sicherung einzelner Gefährdungsbereiche stellt meist die wichtigste Abwehrmaßnahme dar, da mit den „äußeren" Maßnahmen, die den gesamten Betriebsbereich betreffen, selten ein völlig ausreichender Schutz zu erreichen ist.

So wird zum Beispiel ein Risiko vorsätzlichen Handelns durch Beschäftigte von Maßnahmen zum äußeren Schutz nicht berührt. Auch kann die Zugangskontrolle zum Betriebs- oder Objektbereich (etwa bei Schichtbeginn oder zu Hauptverkehrszeiten) kaum in tatsächlich lückenloser Weise durchgeführt werden. Im Gegensatz hierzu bestehen durchaus Möglichkeiten, an einzelnen Stellen des Betriebsbereichs eine wesentlich wirksamere Kontrolle durchzuführen.

3.3.2 Personal

Grundsätzlich sind Anschläge auf ein Unternehmen sowohl von Außen- als auch von Innentätern durchführbar. Während Konzepte zum Schutz gegen Eingriffe von außen in nicht unerheblicher Anzahl existieren, besteht für den Bereich möglicher Gefährdungen durch Innentäter verstärkter Handlungsbedarf. Hierunter werden Beschäftigte des eigenen Unternehmens oder Fremde verstanden, die sich befugt im Bereich sicherungsrelevanter Anlagen aufhalten, aber unbefugte Eingriffe vornehmen. Sie können über gute Kenntnis der entsprechenden Anlagen verfügen und dies in krimineller Absicht nutzen wollen.

Sensibilisierung des Personals

Hinsichtlich der Abwehrmaßnahmen sind sowohl der Staat als Garant der Inneren Sicherheit als auch die Betreiber von Infrastruktureinrichtungen in der Pflicht. Dabei sind neben den allgemeinen Maßnahmen der Sicherheitsbehörden auch präventive Maßnahmen der Betreiber erforderlich. Diese sind vor allem dem Bereich der Personalführung und -überwachung zuzuordnen (Erzeugung einer Identifikation mit dem Unternehmen, Motivation, sensibler Umgang mit belastenden Personalmaßnahmen, Schulung der Vorgesetzten etc.). Darüber hinaus sollte eine allgemeine Sensibilisierung aller Beschäftigten gegenüber diesem Problemkreis geschaffen werden. Eine Beratung durch besonders qualifizierte Spezialisten kann sinnvoll sein. Ebenso sollte von der Möglichkeit einer Sicherheitsüberprüfung von Beschäftigten in hochsensiblen Bereichen Gebrauch gemacht werden. Für eine erste Analyse sollten

Informationen über die Anzahl anwesender Leasingkräfte oder Fremdfirmenmitarbeiter und Angaben über deren Bindung an den Betriebsbereich (insbesondere Dauer der Zusammenarbeit) sowie über die durchschnittliche Anzahl von Besuchern vorhanden sein. Weitere Hinweise über präventive Maßnahmen im Bereich Personal erteilen die zuständigen Behörden, insbesondere die Polizeidienststellen, die Landeskriminalämter, das Bundeskriminalamt sowie die Landesämter und das Bundesamt für Verfassungsschutz.

3.3.3 Organisation und Management

Die interne Organisation, insbesondere ablauforganisatorische Maßnahmen, sowie das Management bilden einen wichtigen Rahmen, in den unterschiedliche Einzelmaßnahmen eingepasst und regelmäßig überprüft werden müssen, damit eine zweifelsfreie Funktion der Gesamtsicherung gewährleistet ist. In diesem Zusammenhang sollte behandelt werden

Betriebliche Ablauforganisation

- das betriebliche Ausweiswesen mit Ausweisausgabe und -rückgabe, Ausweiskodierung (Art und Abwicklung), Ausweisaufbewahrung (Sicherung vor Zugriff), Zuständigkeiten (analog auch für Kennworte beziehungsweise elektronische Zugangsrechte),
- das Einstellungs- und Überwachungsverfahren für Personal mit Sicherungsaufgaben, Zugangserlaubnis zu gefährdeten Stellen und Arbeitsplätzen,
- die Ausbildung, Unterweisung und das Training von Personen zum Beispiel zum Vermeiden von Fehlbedienungen,
- Regeln der Aufsicht und regelmäßige Kontrollen bei Arbeiten in sicherungsrelevanten Bereichen,
- das Schlüsselwesen im Einzelnen mit Schließsystem (Art, Umfang, Alter), Schlüsselausgabe, -rückgabe und -registrierung sowie Schlüssel- und Zylinderaufbewahrung,
- die Reinigung in sicherungsrelevanten Bereichen mit Eigen- oder Fremdkräften, Reinigungszeiten, Aufsicht bei der Reinigung, Personalkontrolle (bei Fremdpersonal),
- die Auflistung von Dienstanweisungen für alle im Zusammenhang mit der Sicherung stehenden Maßnahmen,
- Alarmpläne für Brände oder Explosionen, Leckagen, Umweltgefährdungen, anlagenspezifische Ereignisse, Geiselnahme, Erpressung usw.,
- die regelmäßige Überprüfung und Aktualisierung des Basisschutzkonzeptes, insbesondere des Schutzbedarfes, der Sicherungsziele und des Maßnahmenkatalogs.

3.4 Risikomanagement

Risikomanagement-kreislauf

Risikomanagementsysteme als Instrumente zur Erhöhung der Sicherheit eines Unternehmens wurden bislang grundsätzlich auf freiwilliger Basis eingerichtet. Mit der Änderung des Aktiengesetzes (§ 91 Abs. 2) sind nun bestimmte Unternehmen zur Einrichtung eines Überwachungssystems verpflichtet worden, um „den Fortbestand der Gesellschaft gefährdende Entwicklungen“ frühzeitig zu erkennen. Grundlage von Risikomanagementsystemen ist die Definition einer Risikopolitik als Bestandteil der unternehmerischen Geschäftspolitik, die Leitlinien zum Umgang mit Risiken festlegt. Risikomanagementsysteme werden in der Regel anhand des Phasenmodells Risikoanalyse, Risikosteuerung und -bewältigung, Risikoüberwachung und Risikofinanzierung erstellt, die auf der für das Unternehmen beschlossenen Risikopolitik aufbauen:

- In der Risikoanalyse sind sämtliche für das Unternehmen relevanten Risiken einschließlich der im Basisschutzkonzept beschriebenen Gefährdungen zu identifizieren, zu analysieren und für jedes Unternehmen individuell zu bewerten.
- Die Risikosteuerung dient der Risikovermeidung oder -minderung und der Risikoabwälzung auf Dritte (Kunden, Versicherungen etc.); ein Restrisiko wird akzeptiert werden müssen.
- Im Rahmen der Risikoüberwachung sind Frühwarn- und Controllingsysteme einzurichten und die Risikopolitik des Unternehmens ist gegebenenfalls anzupassen.

- Von großer Bedeutung für Unternehmen ist die Frage der Risikofinanzierung, wobei hier mittel- bis langfristige Überlegungen im Vordergrund stehen müssen, um die Vorteile der Investition in Sicherheit, etwa im Wettbewerb, angemessen beurteilen zu können.

Die Einführung von Risikomanagementsystemen kann in institutioneller Hinsicht durch die Ernennung eines Risikobeauftragten unterstützt werden, der gemeinsam mit den für die Sicherheit zuständigen Beauftragten im Unternehmen, aber auch mit den zuständigen (behördlichen und nichtbehördlichen) Stellen außerhalb des Unternehmens ein Risikomanagementsystem konzipiert und veränderten Rahmenbedingungen kontinuierlich anpasst.

3.4.1 Notfallplanung

Für den Fall einer Beeinträchtigung oder (Zer-)Störung der Infrastruktureinrichtung haben die Betreiber Maßnahmen zu ergreifen, um deren Auswirkungen so gering wie möglich zu halten. Um die Folgen einer Störung oder Krise auf Kritische Infrastrukturen beherrschen zu können, müssen Informationen über die Einrichtungen ebenso wie über vorgenommene und geplante Maßnahmen auch den Gefahrenabwehrbehörden vorliegen. Diese wiederum müssen die Szenarien in entsprechende eigene Alarm- und Gefahrenabwehrpläne umsetzen. Hinsichtlich der auswirkungsbegrenzenden Maßnahmen werden folgende Empfehlungen ausgesprochen:

Kooperation mit Gefahrenabwehrbehörden

- Auch Betreiber von Anlagen und Objekten, die nicht erweiterten gesetzlichen Pflichten wie zum Beispiel der Störfallverordnung unterliegen, die sich aber als sicherungsrelevant erwiesen haben, sollen sich auch aus eigenem Interesse unverzüglich mit den Gefahrenabwehrbehörden in Verbindung setzen und die nötigen Informationen zur Erstellung externer Alarm- und Gefahrenabwehrpläne übermitteln. Die Immissionsschutz- und Gefahrenabwehrbehörden sollen sich zwecks Identifizierung dieser möglichen relevanten Anlagen untereinander verständigen.
- Die zuständigen Gefahrenabwehrbehörden sollen auf der Grundlage der vorhandenen Informationen der Betreiber zum Schutze der Bevölkerung unverzüglich die notwendigen externen Alarm- und Gefahrenabwehrpläne erstellen.
- Für den Katastrophenfall sollten Maßnahmenpläne erstellt und regelmäßig aktualisiert werden (zum Beispiel Telefonlisten, Zuweisung von Verantwortung, Ablaufpläne). Hierzu gehören auch Vorbereitungen für eine funktionierende und effektive Krisenkommunikation.
- Ein Meldezentrum sollte eingerichtet werden. Hierzu wird Personal benannt und vorgehalten, das im Krisenfall zusammentritt. Weiterhin werden Räumlichkeiten benötigt, die gegen äußere Einflüsse zu sichern sind und mit funktionierenden Kommunikationsmitteln ausgestattet werden sollten.

Darüber hinaus wird die Erstellung, Umsetzung und regelmäßige Prüfung von Notfallkonzepten für einen möglichen Personalausfall empfohlen.

3.4.2 Risiko- und Krisenkommunikation

Sowohl im Vorfeld möglicher Krisenereignisse als auch besonders nach Eintritt schwerer Schadensfälle mit Bezug zu Kritischen Infrastrukturen kommt einer angemessenen und möglichst effizienten Kommunikation eine herausgehobene Bedeutung zu. Hierzu sollte ein Kommunikationskonzept vorliegen, das beispielsweise folgende Elemente umfasst:

Krisenkommunikation

- Bereits vor einem niemals gänzlich auszuschließenden Krisenfall müssen geeignete Kommunikationsformen gefunden und gefördert werden, um im Ereignisfall die Medien und die Bevölkerung zu informieren und zu sensibilisieren.
- Da ein vollständiger Schutz nie gewährleistet werden kann, kommt auch bereits im Vorfeld den Maßnahmen der außerbetrieblichen Gefahrenabwehr besondere Bedeutung zu. Die hierfür zuständigen Behörden müssen von den Betreibern die erforderlichen Informationen erhalten und die in

ihrer Zuständigkeit liegenden Maßnahmen treffen. Die für die Einschätzung der Gefährdungssituation durch die Betreiber und die Behörden erforderlichen Informationen müssen zu einem erheblichen Teil aufgrund der Vorschriften zum Sicherheitsbericht (§ 9 StörfallV) sowie zu den Alarm- und Gefahrenabwehrplänen (§ 10 StörfallV, Landesgesetze zum Brand- und Katastrophenschutz) vorhanden sein. Für Einrichtungen Kritischer Infrastrukturen, die nicht der Störfallverordnung unterliegen, sollten sie als wesentlicher Bestandteil eines integrativen Sicherungsmanagements in vergleichbarer Weise erhoben und dokumentiert werden.

Koordination der Kommunikationswege

- Im Krisenfall sind zeitnahes Handeln und Kommunizieren von entscheidender Bedeutung. Dabei müssen der öffentliche und der private Sektor koordiniert und einsatzorientiert reagieren. Hier sollte vorab definiert sein, wie im Krisenfall nach innen und nach außen kommuniziert wird, unter besonderer Berücksichtigung der elektronischen Medien (und ihres eventuellen Ausfalls). Es sollte festgelegt werden, wie über E-Mail, Webseiten, klassische und Mobiltelefonie sowie über Funk kommuniziert wird, einschließlich einer Festlegung zentraler Informationsflüsse und Meldewege. Auch der Analyse der (globalen) Medienlage kommt in diesem Zusammenhang besondere Bedeutung zu, denn in vielen Fällen kann die psychologische Wirkung an sich begrenzte Ereignisse dramatisieren.
- Besonders zu betrachten sind Teile des Unternehmens (zum Beispiel Anlagen), bei denen im Bereich besonders schutzwürdiger Objekte das Leben von Menschen bedroht wird oder schwerwiegende Gesundheitsbeeinträchtigungen von Menschen zu befürchten sind. Diese Informationen sind unter anderem Voraussetzung für eine effiziente Kommunikation mit staatlichen Stellen und sollten auch Bestandteil des betrieblichen Basisschutzkonzeptes sein.

Risikokommunikation: Veröffentlichung sensibler Daten

- Hinsichtlich eventueller Bedenken bezüglich der Veröffentlichung von sensiblen Daten bedarf es im Einzelfall einer sorgfältigen Abwägung der betroffenen Rechtsgüter. Weiter ist zu beachten, dass die Information Dritter über sie betreffende Risiken nicht nur ein Freiheitsrecht darstellt, sondern auch ein Element der Vorsorge ist. Neben der Abwägung der Rechtsgüter bedarf es daher der Entwicklung von Kriterien, um den möglichen Verlust an Sicherheit gegen einen möglichen Gewinn an Sicherung abzuwägen.

3.4.3 Ausfallplanung und Business Continuity Management

Vorsorgemaßnahme Ausfallplanung

Um den Geschäftsbetrieb auch im Krisenfall weitgehend aufrechterhalten, zumindest jedoch einen Notbetrieb einrichten und möglichst schnell die vollständige Funktionsfähigkeit wieder erreichen zu können, müssen frühzeitig Konzepte einer Ausfallplanung und Maßnahmen im Rahmen der Business Continuity festgelegt werden. Ausfall- und Wiederanlaufplanung als Vorsorgemaßnahmen gehen über das unmittelbare Notfallmanagement zur Bewältigung der aktuellen Krise hinaus; die Erstellung dieser zentralen Instrumente der Krisenbewältigung bedarf der Initiierung und Begleitung durch das oberste Management. Ausfallpläne sollten insbesondere Alternativkonzepte zur Gestaltung zentraler Geschäftsprozesse bei Ausfall von kritischen Bereichen im Unternehmen sowie von Zulieferern und Dienstleistern berücksichtigen, aber auch die Bereitstellung von Redundanzen sowie eines Ausweichstandortes in Betracht ziehen. Zumindest folgende Punkte sind zu berücksichtigen:

- Für besonders sensible Bereiche sollten redundante Systeme bereitgehalten werden (zum Beispiel Notstromversorgung, Datenleitungen, mehrzügige Produktion). Diese sollten aus Sicherheitsgründen räumlich getrennt werden.
- Für den Betrieb der Anlagen ist eine ausreichende Menge an Betriebsstoffen vorzuhalten (zum Beispiel für Produktion, Notstromversorgung und sonstige vitale Prozesse). Hierbei ist besonders auf die Auswirkungen großflächiger Ereignisse, die über mehrere Tage andauern, zu achten (zum Beispiel unpassierbare Zufahrtswege, lang anhaltende Stromausfälle).
- Bei der Planung, aber auch im Betrieb, sollen Aspekte einer fehlertoleranten Gestaltung von Arbeitsmitteln, Anlagen und Prozessen Berücksichtigung finden (Auswirkungsbegrenzung).
- Zum Schutz vor Personalausfall, zum Beispiel durch Epidemien, sollten ausreichende Personalkapazitäten, insbesondere in Schlüsselpositionen, vorgehalten werden. Empfohlen werden die Erstellung, Umsetzung und regelmäßige Prüfung von Notfallkonzepten für einen möglichen Personalausfall.
- Ausfall- und Notfallpläne sind regelmäßig zu überprüfen und neuen Entwicklungen anzupassen.

3.5 Qualitätsmanagement und Dokumentation der Schutzmaßnahmen

3.5.1 Qualitätsmanagement der Schutzmaßnahmen

Integration in bestehendes Qualitäts-managementsystem

Um sicherzustellen, dass auch Schutzmaßnahmen, wie sie beispielsweise im Basisschutzkonzept vorgeschlagen werden, den Anforderungen entsprechend realisiert und in einem ständigen Verbesserungsprozess optimiert werden, sollten die Schutzkonzepte einem Qualitätsmanagement unterzogen werden. Es empfiehlt sich, das Teilkonzept „Qualitätsmanagement der Schutzmaßnahmen“ in ein bestehendes unternehmensinternes Qualitätsmanagementsystem zu integrieren, Zuständigkeiten und Verantwortlichkeiten festzulegen und diese zu dokumentieren. Damit erhält das Qualitätsmanagement im Bereich der Schutzmaßnahmen auch einen festen Platz im Rahmen der Unternehmenspolitik und ist Bestandteil der Aufgaben des Top-Managements.

Für eine erfolgreiche Umsetzung der Schutzmaßnahmen und eine kontinuierliche Überprüfung müssen die Anforderungen klar und eindeutig formuliert werden. Hier bietet sich die Orientierung an den **s.m.a.r.t.**-Kriterien an:

s (spezifisch): Was und wie viel soll genau erreicht werden?
m (messbar): Existieren Messkriterien oder Maßstäbe, an denen die Zielerreichung gemessen und kontrolliert werden kann? Sind Checklisten entsprechend gestaltet?
a (attraktiv, akzeptiert): Ist das Ziel anspruchsvoll, ist die Zielerreichung mit den verfügbaren Mitteln aktiv zu beeinflussen?
r (realistisch, realisierbar): Ist das Ziel unter Berücksichtigung der Umstände und Ressourcen erreichbar?
t (terminiert): Ist eine Frist gesetzt, innerhalb der das Ziel (oder die Zwischenziele) erreicht werden soll?

Regelkreislauf Qualitätsmanagement

Qualitätsmanagement ist kein statischer Prozess, sondern folgt einem Regelkreislauf von Planung, Umsetzung, Analyse und Nachsteuerung, anhand dessen sich ein kontinuierlicher Verbesserungsprozess entwickelt. Daher sind auch die Sicherungsmaßnahmen einer regelmäßigen Überprüfung zu unterziehen und Möglichkeiten der Nachsteuerung bei Abweichungen (zum Beispiel Nachschulungen von Sicherheitspersonal, Anpassung von Prozessen etc.) zu implementieren.

3.5.2 Dokumentation der Schutzmaßnahmen

Im Rahmen eines betrieblichen Basisschutzkonzeptes sollten die Schutzmaßnahmen für jede einzelne Gefährdungsstelle dokumentiert werden, wobei ein Zusammenfassen in Bereiche, Gebäude, Abschnitte oder Funktionseinheiten sinnvoll sein kann. Es versteht sich von selbst, dass gerade diese Ausführungen besonders vertraulich sind. Für einzelne Gefährdungsstellen sollten folgende Aspekte berücksichtigt werden:

- Lage auf dem Betriebsgelände (Lageplan), Lage innerhalb von Gebäuden oder Bereichen (Grundrissplan),
- Zugänge, Zufahrten, Fluchtwege,
- bauliche und mechanische Ausführung bei Bereichsabtrennungen (Mauern, Zäune),
- bauliche Ausführung von Gebäuden und den sicherungsbedeutsamen Räumen (Material, Bewehrung, Wandstärken),
- mechanische Sicherung von Türen, Fenstern und Durchbrüchen,
- elektronische Überwachungsmaßnahmen bei Türen, Fenstern, Räumen etc.,
- Abwicklung der Zugangskontrolle zu den betreffenden Stellen während und nach der Dienstzeit für Personal und Betriebsfremde,

- Sicherung einzelner Bedienungselemente gegen Fehlbedienen oder Sabotage zum Beispiel durch mechanischen Verschluss oder elektronisches Überwachen,
- Anbringung von Hinweis- und Warnschildern,
- besondere Sicherungsmaßnahmen,
- Dienst- und Schichtzeiten der zuständigen Abteilung, gegebenenfalls Unterscheidung von Sicherungsmaßnahmen,
- Bestreifung der Objekte durch den Werkschutz (Streifenwege, Streifenzeiten).

Gefährdungsartentabelle

	Gefährdungsart 1	Gefährdungsart 2	Gefährdungsart 3
Tatabsicht:	Der Verursacher (Straftäter) will einen begrenzten Schaden verursachen; eine weit höhere Gefahrensituation nimmt er billigend in Kauf oder ist ihm nicht bewusst (bedingter Vorsatz)	Der Verursacher (Straftäter) will den Eintritt eines größeren Schadensfalles und eine damit ausgelöste allgemeine Gefährdungslage herbeiführen, auch als Ablenkungsmanöver (direkter Vorsatz)	Der Verursacher (Straftäter) will massive Anschläge mit Fanalwirkung (gemeingefährliche, brutale Vorgehensweise)
Motivation:	Rache, Frustration, Unzulänglichkeiten „nachweisen“, politische Effekte erzielen, Aufmerksamkeit erregen, Schutzgelderpressung	(innen-)politische Radikalität, Rache, Erzielen von erheblichen Vermögens- und Wettbewerbsvorteilen	Anarchismus, Herbeiführen gesellschaftlicher Veränderungen mit Gewalt, „Bestrafen“ von Unternehmen (auch stellvertretend für Staaten) oder Regierungen, glaubensbezogene Motive
Vorbereitungshandlungen:	Ausspähen, Beschaffen von Werkzeugen und anderen Tatmitteln	Erkunden sicherheitsrelevanter Anlagenteile und Schwachstellen, gezieltes Ausnützen von Lücken bei der Überwachung, Beschaffen spezieller Hilfsmittel, Außerbetriebsetzen von Sicherheitseinrichtungen	logistische Vorbereitungen, Ausspähung, Außerbetriebsetzen von Sicherheitsanlagen
Tatmittel:	einfache und schwere Werkzeuge, einfache Brandsätze	einfache und Spezialwerkzeuge, Unkonventionelle Spreng- und Brandvorrichtungen (USBV, Selbstbau)	einfache und Spezialwerkzeuge, USBV, Sprengstoff in großen Mengen, (ABCR-)Waffen, ohne Rücksicht auf (das eigene) Menschenleben
Personenkreis:	außen: radikale Gruppen, im Auftrag handelnde Kriminelle, gewaltbereite Einzeltäter innen: Personal, entlassene, ehemalige Beschäftigte, Fremdfirmenangehörige und Besucher	Einzeltäter, Tätergruppen, auch im Rahmen der „organisierten Kriminalität“, radikale politische Gruppen	extremistische und terroristische Einzeltäter und Gruppen
Anmerkungen/Beispiele:	Außerbetriebsetzen von Sicherheitseinrichtungen, Eingriffe in Produktionsabläufe, Nichtweitermelden kritischer Anlagenzustände, Brandstiftung, Vandalismus nach erfolglosem Einbruch, Brandstiftung aus anderen Motiven	Brand- oder Sprengstoffanschlag, Zerstören von wichtigen Betriebseinrichtungen, Eingriffe in Steuerungsanlagen einschließlich Fehlprogrammierung von Steuerprozessoren	bewaffneter Überfall, Sprengstoffeinsatz an belebten Plätzen, Raketenbeschuss, Inbrandsetzen größerer Anlagen, Angriffe auf Werkschutzpersonal, gezielte Anschläge auf besonders sensible Bereiche, Einsatz biologisch-chemischer Kampfstoffe, radioaktive Verseuchung mit Sprengwirkung („dirty bomb“)

4 Zu kontaktierende

Behörden und Institutionen

Besonders wichtig ist neben den möglichen sicherheitstechnischen und organisatorischen Verbesserungen vor allem auch die gute und intensive Zusammenarbeit zwischen den Betreibern Kritischer Infrastrukturen und den Sicherheits- und Gefahrenabwehrbehörden.

Im Rahmen des Basisschutzes sollte eine Abstimmung mit den zuständigen Behörden und Institutionen erfolgen, um diese wirkungsvoll auch in die Informationsgewinnung für Risiken und die Auswahl geeigneter Maßnahmen einzubinden. Mit Blick auf Gefährdungen durch natürliche Ereignisse sowie durch menschliches oder technisches Versagen sind beispielsweise Behörden und Anstalten für Raumordnung und Raumplanung sowie für Geologie und Wetterinformationen, Katastrophen- und Brandschutzämter, Regulierungsbehörden, Ordnungs- und Baubehörden, Immissionsschutzämter, Gesundheitsbehörden sowie Umweltbehörden frühzeitig zu kontaktieren. Unmittelbarere Ansprechpartner für Unternehmen und Betreiber Kritischer Infrastrukturen sind zunächst die Behörden auf kommunaler Ebene sowie die Landesbehörden.

Für den Bund nimmt das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) Aufgaben auf den Gebieten des Bevölkerungsschutzes und der Katastrophenhilfe wahr. Das BBK verknüpft fachübergreifend alle Bereiche der zivilen Sicherheitsvorsorge zu einem wirksamen Schutzsystem für die Bevölkerung und ihre Lebensgrundlagen. Das Zentrum Schutz Kritischer Infrastrukturen im BBK hat als „Netzknoten“ unter anderem die Aufgabe, über die Bedeutung von Kritischen Infrastrukturen für Staat und Gesellschaft zu informieren und zu sensibilisieren, Kooperationen zwischen Behörden und Unternehmen aufzubauen, Analyse- und Schutzkonzepte zu entwickeln sowie kurz-, mittel- und langfristige Maßnahmen zum Schutz Kritischer Infrastrukturen vorzuschlagen.

Die Bundesanstalt Technisches Hilfswerk (THW) leistet technische Hilfe im Zivilschutz sowie bei der Bekämpfung von Katastrophen, öffentlichen Notständen und Unglücksfällen größeren Ausmaßes. Das THW wird auf Anforderung der für die Gefahrenabwehr zuständigen Stellen tätig und erfüllt unter anderem Aufgaben im Rahmen der technischen Gefahrenabwehr, der technischen Hilfe im Bereich der Infrastruktur, der technischen Hilfe im Umweltschutz sowie der Versorgung der Bevölkerung in Katastrophenfällen.

Soweit zum Schutz vor Eingriffen Unbefugter externe Unterstützung, zum Beispiel durch die Polizei, erforderlich ist, sollte der Betreiber bereits im Vorfeld möglicher Eingriffe den Kontakt zu den zuständigen örtlichen Behörden aufnehmen.

Grundsätzlich sind hier im Rahmen der Gefahrenabwehr und präventiven Maßnahmen wie auch im Falle konkreter Ermittlungen ebenfalls die Länder zuständig. Im Bereich der Sicherung von Bahnanlagen, Flughäfen und Grenzen ist die Bundespolizei (vormals Bundesgrenzschutz – BGS) der Ansprechpartner. Ermittlungszuständigkeiten des Bundeskriminalamtes (BKA) sind nur in besonderen Ausnahmefällen gegeben, so etwa in Fällen schwerer Computerkriminalität nach § 303b Strafgesetzbuch, soweit „tatsächliche Anhaltspunkte dafür vorliegen, dass die Tat sich gegen a) die innere oder äußere Sicherheit der Bundesrepublik Deutschland oder b) sicherheitsempfindliche Stellen von lebenswichtigen Einrichtungen, bei deren Ausfall oder Zerstörung eine erhebliche Bedrohung für die Gesundheit oder das Leben von Menschen zu befürchten ist oder die für das Funktionieren des Gemeinwesens

unverzichtbar sind, richtet." In besonderen Lagen ist das BKA auch dann an Ermittlungen beteiligt, wenn es zwar nicht aufgrund von § 4 des Gesetzes über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (Bundeskriminalamtgesetz – BKAG) zuständig ist, aber zum Beispiel durch Politik oder Generalbundesanwalt damit beauftragt wird.

Speziell mit Fragen der IT-Sicherheit in der Informationsgesellschaft befasst sich das Bundesamt für Sicherheit in der Informationstechnik (BSI). Als zentraler IT-Sicherheitsdienstleister des Bundes informiert das BSI über Risiken und Gefahren beim Einsatz der Informationstechnik, entwickelt unter anderem Kriterien und Verfahren für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen und berät neben Herstellern und Vertreibern auch Anwender in Fragen rund um die Sicherheit in der Informationstechnik.

Anhang 1

Fragenkatalog und Muster für eine Checkliste

Das Basisschutzkonzept kann nur umgesetzt werden, wenn theoretische Erkenntnisse über Gefahren, Bedrohungen und Risiken mittels entsprechender Managementkonzepte operationalisiert werden. International setzen sich als Hilfsmittel für die Operationalisierung von Sicherheitskonzepten zunehmend Fragenkataloge sowie einfach abzuarbeitende Checklisten durch.

Der hier vorgelegte Fragenkatalog und die Checkliste sind als Muster zu verstehen, um das Basisschutzkonzept eigenverantwortlich sowie praxis- und anwenderorientiert umzusetzen. Die Fragen sollen vor allem dazu dienen, einen unternehmensinternen Diskussionsprozess über die Erhöhung der Sicherheit zu initiieren und zielgerichtet zu steuern. Die Checklisten sollen als konkretes Hilfs- und Kontrollinstrument im Rahmen der Umsetzung dienen.

Fragenkatalog

Der Fragenkatalog hat keinen abschließenden Charakter, sondern ist ebenso wie das Muster für eine Checkliste im Kooperationsprozess zu vervollständigen und weiterzuentwickeln.

I. Strukturen und Kooperationen (Organisation und Management)

1. Wie ist die Konzernsicherheit des Unternehmens strukturiert und ausgestattet? Welche Beziehungen oder Kooperationsstrukturen zwischen materieller Sicherheit, IT-Sicherheit und personeller Sicherheit existieren beziehungsweise sind geplant?
2. Wie arbeitet das Unternehmen im Sicherheitsbereich mit anderen Unternehmen zusammen, einschließlich anderen Nutzern der Infrastruktur beispielsweise in regionalen Verbünden und privaten Anbietern von auszulagernden Dienstleistungen (Outsourcing)?
3. Welche Sicherheitsmaßnahmen und Kooperationsstrukturen im Bereich vor- und nachgelagerter Teile der Wertschöpfungsketten existieren oder sind geplant? Welche weiteren Kooperationen bestehen für den Großschadensfall? Wie ist die Zusammenarbeit mit den beteiligten Sicherheitsbehörden sowie Rettungs- und Katastrophenschutzorganisationen geregelt und wie wird sie evaluiert?
4. Welche Einrichtungen des Unternehmens, der Branche oder der Aufsichtsbehörden oder welche externen Einrichtungen befassen sich mit der Analyse von Schadensfällen (Rekonstruktion der Schadensursache, Schlussfolgerungen, Umsetzung einschließlich Erfolgskontrolle) und, darauf basierend, der Weiterentwicklung zum Beispiel im Bereich der technischen Sicherheit?

II. Untersuchungen, Konzepte (Analyse des Schutzbedarfs)

5. Welche speziellen Sicherheitskonzeptionen für besonders sensible Bereiche existieren? Nach welchen Kriterien werden solche Bereiche identifiziert beziehungsweise eingestuft? Wurde ein

Schutzniveau ermittelt? Zu welchen Aussagen gelangen vergleichende Untersuchungen bezüglich internationaler Konzepte und Entwicklungen?

6. Welche Untersuchungen und Konzepte bezüglich der Substitution von Dienstleistungen bei Großschadenslagen existieren?
7. Welche Ansätze bezüglich Qualitätsmanagement und Risikomanagement werden verwendet und wie sind die Erfahrungen damit? Welche Bedeutung hat das Sicherungsmanagement im unternehmerischen Optimierungsprozess?
8. Welche Risikoanalysen liegen vor, wer hat sie beauftragt und durchgeführt? Welche Konzepte für eine intensivierte und systemübergreifende Analyse und Maßnahmenentwicklung bezüglich Interdependenzen existieren?
9. Werden Kosten-Nutzen-Analysen hinsichtlich der Verwendung und Einführung von Sicherheitsmaßnahmen durchgeführt?
10. Welche Zwischenfälle werden erfasst? Welche Aussagen zu nicht erfassten Zwischenfällen (Dunkelfeld) sind möglich?

III. Präventionsmaßnahmen (innerer, äußerer und personeller Schutz)

11. Welche herausragenden Konsequenzen aus besonders gravierenden Vorfällen im Zusammenhang mit dem Kerngeschäftsfeld des Unternehmens wurden in der Vergangenheit gezogen (gegebenenfalls auch weltweit)?
12. Welche Instrumente der technischen Überwachung, der Ermittlungen und der Beweissicherung werden genutzt? Wie haben sich die Maßnahmen bewährt?
13. Mit welchen technischen und organisatorischen Maßnahmen sind a) die Produkte und b) die Produktionsprozesse und -anlagen gegen Missbrauch gesichert?

IV. Krisenmanagement bei Großschadenslagen (Ausfallplanung, Redundanzen, Notfallpläne)

14. Wie erfolgt die Vorfallsbehandlung, beispielsweise Eskalationswege, Risikobewertung, Entscheidungsbefugnisse etc.? Existieren sektorspezifische Ansätze und Handlungsanleitungen zur Differenzierung von Schadenslagen beziehungsweise der Vorfallsbehandlung?
15. Welcher Optimierungsbedarf a) aus Sicht der und b) an die Behörden und Organisationen mit Sicherheitsaufgaben (BOS) besteht hinsichtlich der Handlungsfähigkeit bei Großschadenslagen?
16. Welche Übungen zur Bewältigung von Großschadenslagen wurden bisher durchgeführt oder sind geplant?

Muster für eine Checkliste Basisschutz

Wie der Fragenkatalog soll auch die folgende Checkliste als konkretes Hilfsinstrument für die Umsetzung des Basisschutzkonzeptes dienen.

Da jedoch individuelle orts- und fachspezifische Besonderheiten nicht berücksichtigt werden können, müssen die hier abgefragten Aspekte an die jeweiligen spezifischen Bedürfnisse angepasst und gegebenenfalls ergänzt werden; ebenso sind unter Umständen weiterführende Sicherheitsmaßnahmen unerlässlich. Insoweit handelt es sich auch bei der Checkliste lediglich um ein Muster ohne abschließenden Charakter.

Die Checkliste umfasst Schutzmaßnahmen für folgende Bereiche:

1. Objektschutz
2. Personal
3. Organisation
4. Risikomanagement
5. Notfallplanung und Ausfallplanung

Objektschutz (Lage des Objekts, bauliche Gestaltung, Vorfeldsicherung, Gebäudesicherung)				
	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Lage des Objekts				
Kann eine Bedrohung des Unternehmens durch schwere Naturereignisse ausgeschlossen werden? – Hochwasser				
– Sturmflut				
– Erdbeben				
– Erd- und Hangrutschungen				
– Lawinen				
– Stürme				
– ...				
Ist die Umgebung um das Unternehmen übersichtlich und ist der Abstand zu den Nachbargebäuden ausreichend, um ein unbefugtes Eindringen feststellen zu können (offene Bauweise)?				
Falls nicht, ist das Unternehmen gegen angrenzende, fremde Gebäude derart abgeschirmt, dass der unbefugte Zutritt (zum Beispiel Einsteigen über angrenzende Dächer) erschwert wird (geschlossene Bauweise)?				
Bauliche Gestaltung				
Ist das Unternehmensgelände verkehrstechnisch gut erschlossen und verfügt über eine Haupt- und davon unabhängige Notausfahrt(en)?				
Ist das Gelände baulich gegen unbefugtes und gewaltsames Eindringen gesichert? – Poller				
– Betonelemente				
– Schranken				
– ...				
Befinden sich Publikumsparkplätze außerhalb des Geländes (öffentlicher Bereich)?				
Wenn ja, ist der Abstand zu den zu schützenden Gebäuden ausreichend?				
Befinden sich schützenswerte Gebäudeteile außerhalb exponierter Lagen und besonders gefährdeter Bereiche?				
Sind die Gebäudefassaden glatt und haben keine Vorsprünge?				
Sind Blitzableiter und andere Anbauten so montiert, dass sie nicht als Aufstieghilfen genutzt werden können?				
Sind Regenwasserfallrohre unter Putz verlegt beziehungsweise verblendet?				
Sind Leitungen und Versorgungsanschlüsse (zum Beispiel Strom, Öl, Gas, Wasser, Telefon) unterirdisch verlegt und manipulationssicher ausgeführt?				
Sind Außensteckdosen schaltbar?				
Vorfeldsicherung				
Ist das Unternehmensgelände eingefriedet?				
Ist die Einfriedung lückenlos?				
Verläuft die Einfriedung geradlinig?				
Ist die Umfriedung relativ durchbruchsicher?				
Ist die Einfriedung frei von Aufstieg- oder Überstieghilfen (zum Beispiel Querstreben, angrenzende Bäume)?				
Hat die Einfriedung eine ausreichende Mindesthöhe?				
Existiert zusätzlich ein Übersteigschutz (zum Beispiel Ausleger mit Stachelband oder Stacheldraht)?				
Falls die Einfriedung mittels Zäunen erfolgt, existiert ein Unterkriechschutz?				
Wenn ja, ist dieser so errichtet, dass er nicht als Aufstieghilfe genutzt werden kann (zum Beispiel Betonsockel oder Betonrandsteine)?				

	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Entsprechen Tore und Türen innerhalb der Einfriedung (zum Beispiel des Zaunes) der Höhe und dem Widerstandswert der Einfriedung?				
Bestehen technische Zufahrtskontrollen (zum Beispiel durch Schiebe-/Flügeltor mit Übersteigschutz, gegebenenfalls mit Schleusenfunktion [Doppeltor], Ausweisleser und/oder Tastaturcode, Videotechnik, Gegensprechanlage)?				
Erfolgt bei Überwindungsversuch der Umfriedung/Zugänge/Zufahrten eine automatische elektronische Detektion (zum Beispiel durch Alarmzäune/Alarmtore, Videotechnik mit Sensorik, Mauerkronensicherungen, Radarsichtstrecken, Hochfrequenzlichtschranken, Einbruchmeldetechnik)?				
Existiert eine schlagschattenfreie Außenbeleuchtung?				
Sind die Beleuchtungskörper gegen Beschädigung geschützt (zum Beispiel mittels durchwurfhemmender Verglasung oder engmaschiger Drahtkörbe)?				
Erfolgt die Stromversorgung der Außenbeleuchtung über Erdkabel?				
Erfolgt eine Überwachung der Einfriedung mittels Videokameras?				
Wenn ja, verfügt das Unternehmen über entsprechend geschultes, handlungsfähiges Wachpersonal zur Kontrolle der Videomonitore?				
Falls Wachpersonal vorhanden ist, werden von diesem auch Bestreifungen durchgeführt?				
Werden Wärmebildkameras/Nachtsichtgeräte eingesetzt?				
Werden neuralgische Stellen/Gebäude(-teile) zusätzlich bestreift?				
Ist die Grundstücksbepflanzung (insbesondere Bäume, hohe Sträucher) weit genug von Türen, Treppen, Erdgeschoss und Kellerfenstern entfernt?				
Gebäudesicherung				
Besteht Sichtschutz von außen für sensible Stellen der Gebäude?				
Wird auf Lagehinweise zu schützenswerten Gebäudeteilen verzichtet (zum Beispiel Wegweiser, Türschilder)?				
Sind innerhalb des Objektes gesonderte Sicherheitsbereiche erforderlich?				
Sind diese Bereiche elektronisch und mechanisch ausreichend gesichert?				
Wurden für diese Bereiche gesonderte Zutrittsbefugnisse ausgearbeitet (Schließkonzept, technische Zutrittskontrolle)?				
Werden Betreten und Verlassen von sensiblen Stellen gesondert überwacht?				
Sind Außentüren, zugängliche Fenster und Lichtschächte in eine Einbruchmeldeanlage integriert?				
Sind Kellerfenster mit geprüften Sicherheitsgittern (mindestens Widerstandsklasse 5 gemäß DIN 18106) versehen?				
Sind Lichtschächte mit stabilen Abdeckgittern und abschließbaren oder fest verschraubten Hochhebesicherungen versehen?				
Sind Öffnungen von Ver- und Entsorgungsschächten, deren Durchmesser größer als 30 cm ist, mit Gittern versehen?				
Sind Dach-/Lichtkuppeln mechanisch und elektronisch gesichert?				
Verfügen die Gebäude über geprüfte einbruchhemmende Fenster (gemäß DIN ENV 1627)?				
Sind die Fenster von Toiletten und anderen Räumen, in denen sich die Fenster erfahrungsgemäß oft in der Kippstellung befinden, vergittert?				
Handelt es sich bei den Fenstern um Sicherheitsglas (durchwurfhemmende A-Verglasung, einbruchhemmende B-Verglasung, beschusshemmende C-Verglasung oder sprengstoffhemmende D-Verglasung)?				

	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Sind nicht vergitterte Fenster (wenn technisch möglich) mit einbruchhemmenden Beschlägen mindestens der Widerstandsklasse WK 5, durchwurfhemmendem Verbundsicherheitsglas (gemäß DIN EN 356, Widerstandsklasse P 6 A), abschließbaren Fenstergriffen und verschraubten Glashalteleisten versehen?				
Ist die Anzahl nach außen führender Türen auf ein sinnvolles Maß beschränkt?				
Entsprechen alle Außentüren mindestens der Widerstandsklasse WK 5 gemäß DIN ENV 1627?				
Verfügt die Tür des Haupteingangs über – Karten- oder Chipleser?				
– kuppelbare, selbstverriegelnde Schlösser?				
– elektrische Sicherheitstüröffner mit einer Druckfestigkeit von mindestens 15000 N?				
– automatische Türschließer?				
– Knauf außen (bei Verwendung von elektrischen Türöffnern)?				
– Videogegensprechanlage?				
Sind Fluchttüren mit selbstverriegelnden Panikschlössern sowie automatischen Türschließern versehen und mit Türwächtern mit örtlichem Alarm ausgestattet?				
Sind der Haupteingang und alle anderen Zugänge auch am Tag ständig verschlossen und nur von berechtigten Personen zu öffnen?				
Ist der Haupteingang mit einer Vereinzelungsanlage (zum Beispiel Drehkreuz oder Drehtürsystem aus Metall oder Glaskonstruktionen) oder einer Schleuse ausgestattet?				
Sind Ein- und Ausgang getrennt?				
Erfolgt die Freigabe für Berechtigte über elektronische Zutrittsberechtigungen (Karten, Transponder)?				
Falls ja, ist die Herstellung, Aufbewahrung, Verwaltung und Ausgabe der elektronischen Zutrittsberechtigungen zentral geregelt?				
Ist eine einfache Zuordnung der Karte zum Unternehmen ausgeschlossen?				
Erfolgt die Vergabe [einer Vielzahl] von Schlüsseln ausschließlich an Berechtigte?				
Ist die Herstellung, Aufbewahrung, Verwaltung und Ausgabe von Schlüsseln zentral geregelt?				
Können Ersatzschlüssel nur nach Vorlage einer Sicherungskarte beim Fachhandel bezogen werden?				
Werden Reserveschlüssel sicher aufbewahrt?				
Werden elektronische Zutrittsberechtigungen beziehungsweise Schlüssel nur gegen Quittung (und Dokumentation) ausgegeben?				
Erfolgt bei Zuständigkeitsänderung oder Ausscheiden von Beschäftigten eine zeitnahe Überprüfung der Schließberechtigungen?				
Brandschutz				
Gibt es eine Blitzschutzanlage (äußerer Blitzschutz) gemäß DIN/VDE 0185?				
Werden bestehende Brandschutzvorschriften (zum Beispiel DIN 4102) und die Auflagen der Bauaufsicht für Gebäude eingehalten?				
Wurde die örtliche Feuerwehr bei der Brandschutzplanung hinzugezogen?				
Existiert eine Gefahrenmeldeanlage, deren Meldungen/Alarm an eine ständig besetzte Stelle (Empfang, Pforte, Wach- und Sicherheitsdienst, Feuerwehr etc.) weitergeleitet wird?				
Weitere Schutzmaßnahmen				

Personal (Beschäftigte, Fremdpersonen)				
	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Personal (intern und extern)				
Wird bei Einstellung neuer Mitarbeiterinnen und Mitarbeiter eine Sicherheitsüberprüfung durchgeführt?				
Wird bei (temporärer) Beschäftigung Externer eine Sicherheitsüberprüfung durchgeführt?				
Werden Sicherheitsüberprüfungen zum personellen Sabotageschutz nach SÜG durchgeführt?				
Wird das Personal zur Einhaltung einschlägiger Gesetze, Vorschriften und interner Regelungen (zum Beispiel § 5 BDSG „Datengeheimnis“) verpflichtet?				
Ist das Personal für Sicherheitsfragen (Terrorismus, Sabotage) sensibilisiert?				
Fremdpersonen[4]				
Müssen sich Fremdpersonen beim Empfang/bei der Pforte/bei der Wache anmelden?				
Sind Fremdpersonen schnell und einfach identifizierbar (zum Beispiel mittels Besucherausweisen)?				
Werden Fremdpersonen begleitet/beaufsichtigt?				
Erfolgt eine Anlieferer- und Warenkontrolle?				
Weitere Schutzmaßnahmen				

[4] Fremdpersonen: z. B. Besucher, Handwerker, Wartungs- und Reinigungspersonal.

Organisation (unternehmensintern, unternehmensextern)				
	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Unternehmensintern				
Gibt es im Unternehmen einen entsprechend geschulten Sicherheitsbeauftragten?				
Wird das Schutzobjekt durch betriebszugehöriges Sicherheitspersonal betreut?				
Ist das betriebszugehörige Sicherheitspersonal mit den für die Ausübung seiner Aufgaben notwendigen rechtlichen Vorschriften und fachspezifischen Pflichten und Befugnissen sowie deren praktischer Anwendung vertraut (etwa durch Unterrichtung analog zu § 34a GewO/§ 4 BewachV)?				
Besteht Klarheit über die sicherheitsrelevanten gesetzlichen Anforderungen und/oder Normen?				
Sind Sicherheitsanforderungen (Leitfäden, Richtlinien) geregelt?				
Wird das Personal über die betrieblichen Sicherheitsanforderungen informiert und regelmäßig geschult?				
Werden sicherheitsrelevante Vorkommnisse aufgezeichnet?				
Wurden Konsequenzen aus sicherheitsrelevanten Vorfällen gezogen?				
Verfügt das Personal über Grundkenntnisse im Bereich Arbeitsschutz, Brandschutz und „Erste Hilfe“?				
Wurden Gefahrenpotenziale und Frühwarnindikatoren identifiziert?				
Gibt es ein Konzept zur Einstufung kritischer Standorte und Unternehmensprozesse?				
Gibt es eine Sicherheitszentrale an Standorten, die als kritisch eingestuft werden?				
Gibt es ein Gefahrstoffkataster im Unternehmen?				
Gibt es genaue Lagepläne aller Ver- und Entsorgungsleitungen (zum Beispiel Strom, (Ab-)Wasser, Gas, Telefon, Gefahrenmeldung)?				
Gibt es Pläne für abgestufte Sicherheitsmaßnahmen (abhängig von der aktuellen Bedrohungslage)?				

	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Gibt es eine Eskalationsstrategie für Sicherheitsvorfälle?				
Gibt es einen Alarmierungsplan?				
Gibt es Verhaltensregeln und Meldewege bei Sicherheitsvorfällen?				
Gibt es regelmäßige Belehrungen über Fluchtwege?				
Gibt es regelmäßige Evakuierungsübungen?				
Gibt es regelmäßige Brandschutzübungen?				
Fließen die Erkenntnisse aus den Übungen in Schulungskonzepte ein?				
Gibt es eine Krisenkommunikation (Information an Beschäftigte, Ansprechpartner für Behörden und Medien)?				
Ist bei sicherheitsrelevanten Vorfällen eine psychologische Betreuung des betroffenen Personals gewährleistet?				
Unternehmensextern				
Gibt es eine so genannte Katastrophenschaltung (Vorrangschaltung für Telekommunikation)?				
Liegt das Sicherheitsmanagement ausschließlich in der Hand des Unternehmens?				
Wenn nein, erfüllen die Vertragspartner/externen Sicherheitsdienstleister DIN 77200 Stufe 3?				
Hat sich dies aus Sicht der Unternehmensführung bewährt?				
Bestehen Vereinbarungen zwischen Unternehmen und Sicherheitsdienstleistern (Vertragsgestaltung, praktische Zusammenarbeit, Zuständigkeiten im Krisenfall)?				
Findet eine objektbezogene Einarbeitung und Weiterbildung des Sicherheitspersonals statt?				
Wurde die Kritikalität von ausgelagerten Dienstleistungen (Outsourcing) für die Funktionsfähigkeit des Unternehmens eingeschätzt?				
Werden Open Sources vermieden, die ein Risiko für das Unternehmen darstellen könnten (zum Beispiel Luftbildaufnahmen im Internet, Produktionsstoffe und -mengen, Distributionswege etc.)?				
Weitere Schutzmaßnahmen				

Risikomanagement	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Ist eine für das gesamte Unternehmen verbindliche Risikopolitik definiert worden?				
Gibt es für Teilbereiche im Unternehmen eine spezifische Risikopolitik?				
Werden alle für das Unternehmen möglichen Risiken erfasst und bewertet, einschließlich der				
– Risiken durch natürliche Ereignisse?				
– Risiken durch menschliches oder technisches Versagen?				
– Risiken durch Terrorismus oder kriminellen Missbrauch?				
Werden Gefahren aus der Umgebung (zum Beispiel Kraftwerke, Eisenbahnlinien etc.) reflektiert?				
Sind der Soll-Sicherheitsstandard und das akzeptierbare Risiko insgesamt und nach Risikoarten definiert?				
Befinden sich alle Risiken im akzeptierbaren Restrisikobereich?				
Bestehen Maßnahmen der Risikobewältigung in allen Teilbereichen (natürliche Ereignisse, menschliches oder technisches Versagen, Terrorismus oder krimineller Handlungen) und sind diese aufeinander abgestimmt?				
Gibt es geeignete Instrumente regelmäßiger Risikoüberwachung (Frühwarnsysteme, Risikocontrolling)?				
Beruhen Entscheidungen der Risikofinanzierung auf mittel- und langfristigen Kosten-/Nutzen-Analysen?				

Notfallplanung und Ausfallplanung	Ja	Nein	Geplant	Handlungsbedarf/ Maßnahmen
Gibt es ein Krisen- und Notfallhandbuch?				
Gibt es eine Regelung der Verantwortung im Notfall?				
Gibt es Krisen- und Notfallpläne für ausgewählte Schadensereignisse?				
Gibt es regelmäßige Notfallübungen?				
Sind Meldewege und Entscheidungsbefugnisse für den Schadensfall organisiert?				
Bestehen für den Großschadensfall Kooperationen mit den zuständigen Behörden?				
Gibt es mit den zuständigen Behörden abgestimmte Krisen- und Notfallpläne?				
Gibt es eine ausreichende Notstromversorgung, die auch die Sicherheitseinrichtungen mit umfasst?				
Sind technische und organisatorische Brandschutzmaßnahmen getroffen?				
– Feuerlöscher				
– Brandmeldeanlagen				
– Schulung des Personals				
– Fluchtwege				
– Überprüfung				
– ...				
Werden Übungen zur Bewältigung von Großschadenslagen (unter Einbindung der zuständigen Behörden) durchgeführt?				
Gibt es einen technischen und organisatorischen Schutz gegen Ausfälle im Produktionsprozess?				
Liegen Untersuchungen und Konzepte zum Ausfall von externen Dienstleistungen bei Großschadenslagen vor?				
Sind Redundanzen vorhanden?				
Gibt es Konzepte zur Wiederaufnahme der Dienstleistung/Produktion nach Schadensfällen (Business-Continuity-Management – BCM)?				
Weitere Schutzmaßnahmen				

II Anhang 2

Hinweise aus polizeilicher Sicht

Es existieren drei Veröffentlichungen, die das Fachreferat „Sprengstoff- und Branddelikte“ des Bundeskriminalamtes (BKA) für die Landeskriminalämter und betroffene Unternehmen erstellt hat. Sie enthalten Hinweise zu Erstmaßnahmen bei Bombendrohungen beziehungsweise zum Verhalten beim Verdacht einer sprengstoffverdächtigen Postsendung oder einer Postsendung mit biologischer oder chemischer Beiladung. Die Veröffentlichungen können bei den zuständigen Landeskriminalämtern angefordert werden (Adressen siehe nebenstehend).

Aufgrund der erheblichen Gefährdung für Personen, die von derartigen Postsendungen ausgeht, sollten bereits im Vorfeld auch Maßnahmen zur Gefahrenminderung eingeplant werden. Dazu gehören neben einem Grundtraining der Mitarbeiter regelmäßige Übungen, festgelegte Verantwortlichkeiten und gegebenenfalls auch bauliche Veränderungen (Stichwort abgesetzte Poststellen).

Hinweis: Wenden Sie sich bei einer Bombendrohung immer an den Polizeinotruf! Grundsätzlich ist jede Bombendrohung ernst zu nehmen und eine abschließende Beurteilung – auf Basis der vom Empfänger der Bombendrohung gesammelten Informationen und Eindrücke – sollte durch die Polizei erfolgen.

Landeskriminalamt
Baden-Württemberg
Taubenheimstraße 85
70372 Stuttgart

Bayerisches Landeskriminalamt
Maillingerstraße 15
80636 München

Landeskriminalamt
Berlin
Platz der Luftbrücke 6
12101 Berlin

Landeskriminalamt
Brandenburg
Tramper Chaussee 1
16225 Eberswalde

Landeskriminalamt
Bremen
In der Vahr 76
28329 Bremen

Landeskriminalamt
Hamburg
Bruno-Georges-Platz 1
22297 Hamburg

Hessisches Landeskriminalamt
Hölderlinstraße 5
65187 Wiesbaden

Landeskriminalamt
Mecklenburg-Vorpommern
Retgendorfer Str. 2
19067 Rampe

Landeskriminalamt
Niedersachsen
Schützenstraße 25
30161 Hannover

Landeskriminalamt
Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf

Landeskriminalamt
Rheinland-Pfalz
Valenciaplatz 1-7
55118 Mainz

Landeskriminalamt Saarland
Hellwigstraße 14
66121 Saarbrücken

Landeskriminalamt
Sachsen
Neuländer Straße 60
01129 Dresden

Landeskriminalamt
Sachsen-Anhalt
Lübecker Straße 53-63
39124 Magdeburg

Landeskriminalamt
Schleswig-Holstein
Mühlenweg 166
24116 Kiel

Landeskriminalamt
Thüringen
Am Schwemmbach
99099 Erfurt

III Anhang 3

Auszug aus:

Für den Notfall vorgesorgt

Eine Information des
Bundesamtes für Bevölkerungsschutz und Katastrophenhilfe

Stand: August 2004

Vollständige Broschüre unter http://www.bbk.bund.de (Themen, Tipps für die Bevölkerung)

Anmerkung:
Die Broschüre „Für den Notfall vorgesorgt“ richtet sich insbesondere an die Bevölkerung und den einzelnen Bürger. Die in der Broschüre vorgehaltenen Informationen zu Gefährdungen durch Naturereignisse und technische Unfälle sowie die Hinweise auf Vorsorgemaßnahmen können in modifizierter Form aber auch für unternehmerische Vorsorgeplanungen genutzt werden.

Inhaltsverzeichnis

Einleitung

Täglich erreichen uns Nachrichten über Unfälle und Katastrophen. Jeder kann von Großbränden, Hochwasser, Chemieunfällen, Stromausfall (Energieausfall) oder anderen plötzlich auftretenden Gefahren betroffen sein.

Für eine umfassende Gefahrenabwehr steht dem Bürger ein umfangreiches Hilfeleistungssystem zur Seite. Während Feuerwehr und Rettungsdienst zur alltäglichen Hilfeleistung bereitstehen, unterhalten die Länder den Katastrophenschutz, um Katastrophen und Gefahren unserer technisierten Umwelt begegnen zu können. Der Bund verstärkt und ergänzt das integrierte Hilfeleistungssystem für großflächige Gefahrenlagen und Krisen durch zusätzliche Fahrzeuge, die Bereitstellung von wehrfreigestellten Helfern, Rettungshubschraubern des Zivilschutzes und das Technische Hilfswerk. Bund, Länder

und Gemeinden arbeiten somit partnerschaftlich im Bevölkerungsschutz zusammen, um Bürgerinnen und Bürgern in einer Notsituation Hilfe zu leisten. Bis Hilfe eintrifft vergeht jedoch Zeit – wertvolle Zeit, in der es vielleicht auf Minuten ankommt, die über das Leben von Menschen oder den Erhalt von Sachwerten entscheiden. Minuten, in denen jeder von uns vielleicht auf sich selbst gestellt ist.

Ist ein Notfall erst eingetreten, ist es für umfangreiche Vorsorgemaßnahmen zu spät, denn gerade dann müssen sie sich ja bewähren. Das richtige Verhalten im Brandfall oder bei Unfällen können wir nicht mehr erlernen, wenn es zu einem Feuer oder einer Verletzung gekommen ist. Helfen können wir nur, wenn wir uns schon vor einem Schadensereignis damit auseinander gesetzt haben, indem wir die erste Hilfe erlernen, sie regelmäßig auffrischen und uns mit den Vorsorgemaßnahmen gegen Gefahrensituationen oder Krisen auseinandersetzen.

Also Vorsorge! Je eher, desto besser, denn niemand kann vorhersagen, wann eine Gefahr ihn selbst betrifft! Oft ist nur wenig Aufwand erforderlich oder wenig Zeit nötig, um eine solide Grundlage für mögliche Notfälle zu schaffen.

Unwettergefahren

Unwetter können so plötzlich auftreten, dass eine Vorbereitung kaum möglich ist. Verfolgen Sie die Wetterberichte und ihre Warnungen. Dies kann Gefahren reduzieren und Schäden vermeiden oder mindern. Bei Unwettern können lose Äste, Bäume und Dachpfannen immer zur Gefahr werden. Bei starken Niederschlägen können Straßen überflutet sein. Schäden in der Straßendecke oder vom Wasserdruck angehobene Kanaldeckel werden somit zu einer Gefahr für Fahrzeuge und Fußgänger. Verständigen Sie die Feuerwehr, wenn gefährliche Substanzen, wie zum Beispiel Heizöl, freigesetzt wurden.

Generell sollten Sie bei Unwettern griffbereit haben:
- ein netzunabhängiges UKW-Radio mit ausreichenden Batterien
- netzunabhängige Lichtquellen wie Taschenlampen und Kerzen
- Notgepäck mit wichtigen Dokumenten, falls Sie ihre Wohnung verlassen müssen.

Tipp: Eine Dokumentation Ihres Eigentums in Form von Fotos oder ähnlichem sollte enthalten sein. Wird Ihr Besitz geschädigt, kann dies für die Versicherung sehr hilfreich sein.

Bei Gewittern, bei denen es zu Blitzentladungen kommt, treten hierdurch zusätzliche Gefahren auf. Beachten Sie hierbei:
- Meiden Sie aufragende Bäume, Masten, Antennen und dergleichen. Suchen Sie Schutz in einem Gebäude.
- Bleiben Sie im Kraftfahrzeug und berühren Sie keine blanken Metallteile.
- Halten Sie zu Überlandleitungen einen Mindestabstand von 50 Metern ein.
- Durch einen Blitz kann es zu Überspannungen kommen. Verlassen Sie sich nicht ausschließlich auf die Blitzschutzanlage Ihres Hauses. Nehmen Sie empfindliche Geräte vom Netz oder verwenden Sie entsprechenden Überspannungsschutz.
- Ein Blitzeinschlag kann Mauerwerk erheblich beschädigen und Risse oder Brüche verursachen.

Hagel und Wirbelstürme sind manchmal eine Folge schwerer Gewitter. Zusätzliche Gefahren sind Hagelkörner sowie Trümmer und Schmutzteile, die durch den heftig rotierenden Schlauch eines Wirbelsturms mitgeführt werden. Bei Hagel und Wirbelsturm sollten Sie zusätzlich beachten:
- Schließen Sie die Roll- oder Fensterläden, halten Sie sich von ungeschützten Öffnungen fern.
- Suchen Sie einen tief liegenden Raum, zum Beispiel Keller oder einen innen liegenden Raum auf; Kraftfahrzeug, Wohnwagen und leichte Gebäude bieten möglicherweise keinen ausreichenden Schutz.
- Meiden Sie Räume mit großer Deckenspannweite wie zum Beispiel Hallen.
- Bleiben Sie nicht im Freien! Suchen Sie ein festes Gebäude auf! Notfalls legen Sie sich mit dem Gesicht erdwärts und schützen Sie Kopf und Nacken mit den Händen!

Verhalten nach einem Unwetter

- Kontrollieren Sie Ihr Umfeld auf Schäden wie Wassereinbruch oder Glasbruch etc.
- Nehmen Sie elektrische Geräte nur in Betrieb, wenn diese nicht mit Feuchtigkeit in Berührung gekommen sind.
- Ist jemand verletzt, leisten Sie erste Hilfe und lösen Sie den Notruf aus.
- Ist das Gebäude beschädigt, so verlassen Sie es und betreten Sie es erst wieder, wenn es von Fachleuten freigegeben wurde.
- Wenn nach einem Sturm das Dach beschädigt wurde, so halten Sie sich aus dem Sturzbereich fern. Er beträgt ein Drittel der Höhe vom Boden zur Dachrinne. Verständigen Sie die Feuerwehr.

Hochwasser

Überschwemmungen haben in den letzten Jahren zunehmend zu einer Bedrohung der Lebensgrundlagen von Teilen der Bevölkerung geführt. Neben den Bemühungen von Bund, Ländern und Gemeinden, die Auswirkungen solcher Schadensereignisse zu begrenzen, sollte auch der Einzelne prüfen, inwieweit er durch gezielte Vorbereitungen und Maßnahmen Schäden vermeiden oder mindern kann. Nachfolgende Hinweise können hierzu beitragen. Sie sollten zuvor die für Ihren Wohnbereich kritische Hochwassermarke über Ihre Kommune abklären.

Bedenken Sie bitte, dass die normale Versorgung mit Strom, Lebensmitteln und Trinkwasser bei Hochwasser beeinträchtigt oder unterbrochen werden kann. Dieser Zustand kann auch nach Ende der unmittelbaren Hochwassergefahr durch die Schädigung der Infrastruktur noch eine Weile anhalten. Besondere Gefahren bei Hochwasser entstehen durch die Kraft des Wassers bei Unterspülung von Wegen, Brücken, Dämmen etc., aber auch durch mitgeführtes Treibgut. Ausgelaufene Schadstoffe wie Heizöl, Reinigungs- und Pflanzenschutzmittel, aber auch Fäkalien und Unrat, die in den Fluten mitgeführt werden, sind ein gesundheitliches Risiko. Trinkwasser kann verunreinigt sein.

Als vorbereitende Maßnahmen empfehlen sich:

- Schalbretter, wasserfeste Sperrholzplatten und Silikon zum Abdichten gefährdeter Räume sowie zusätzlich Sandsäcke bereithalten.
- Gefährliche Stoffe oder Chemikalien rechtzeitig auslagern.
- Wertvolle Möbel oder Geräte aus gefährdeten Räumen auslagern.
- Wasserbeständige Baustoffe verwenden und Versiegelungen in gefährdeten Räumen vornehmen.
- Heizöltank gegen Aufschwimmen sichern (vertikale Rückverankerung/Ballastierung, zum Beispiel durch Erdabdeckung bei drohender Gefahr). Möglichst Tanks verwenden, die für den Lastfall „Wasserdruck von außen“ geeignet sind. Absperrmöglichkeiten von Leitungen vorbereiten.

Zur Sicherheit berücksichtigen:

- Planen Sie die Versorgung hilfebedürftiger oder kranker Personen. Organisieren Sie die Möglichkeit rechtzeitiger „Evakuierung“ zu Verwandten oder Freunden außerhalb der Gefahrenzone.
- Im Gefahrenfall können Festnetztelefon und auch Mobilfunknetz ausfallen, sprechen Sie daher mit Nachbarn und Feuerwehr Not- und Gefahrenzeichen ab.
- Informieren Sie jedes Familienmitglied über getroffene Gefahrenvorsorge, richtiges Verhalten und wichtige Bestandteile der privaten Vorsorge. Sprechen Sie über die „Rollenverteilung“ im Ernstfall (Bedienung von Hauptschaltern und Absperrventilen, Dokumentensicherung etc.).

Bei drohendem Hochwasser:

- Verfolgen Sie aktuelle Wettermeldungen und Hochwasserwarnungen über regionale Rundfunksender und Videotexttafeln regionaler Fernsehsender. Mitbewohner gegebenenfalls zusätzlich informieren.
- Überprüfen und ergänzen Sie getroffene Vorsorgemaßnahmen.
- Räumen Sie gefährdete Räume aus.
- Dichten Sie gefährdete Türen und Fenster, Abflussöffnungen etc. ab.
- Sichern Sie Heizung und elektrische Geräte in bedrohten Räumen beziehungsweise schalten Sie diese ab. Stromschlaggefahr entsteht bereits bei Kondenswasser! Tiefkühltruhe berücksichtigen.
- Überprüfen Sie Hausentwässerungsanlagen und Rückstauklappen im Keller.
- Entfernen Sie rechtzeitig Fahrzeuge aus gefährdeten Garagen oder von Parkplätzen.

- Verständigen Sie bei Austritt von Schadstoffen die Feuerwehr.

Zusätzlicher Hinweis zu Kraftfahrzeugen:
- Befahren Sie keine überfluteten Straßen. Dringt Wasser in den Motorraum, droht erheblicher Schaden; zudem liegt die Betriebstemperatur eines Katalysators bei rund 700°C, plötzliche Abkühlung kann zum Zerspringen des Keramikkopfes führen.
- Steht das Fahrzeug bis zur Ölwanne oder über die Räder im Wasser, starten Sie es keinesfalls, sondern lassen Sie es abschleppen und in einer Werkstatt überprüfen.

Retten Sie Leben:
- Menschenrettung steht vor der Erhaltung von Sachwerten.
- Keine Rettungsversuche ohne Eigensicherung, rufen Sie Hilfe!
- Betreten Sie Uferbereiche wegen der Unterspülungs- und Abbruchgefahr nicht! Dies gilt auch für das Befahren überfluteter oder teilüberfluteter Straßen! Beachten Sie die Absperrungen und folgen Sie den Anweisungen der Gemeinde und der Einsatzkräfte!
- Fahren Sie auf hochwasserführenden Gewässern wegen der Wellenbildung und der Gefahr von Unterwasserhindernissen nicht mit einem Privatboot „spazieren"!

Nach dem Hochwasser
- Entfernen Sie Wasserreste und Schlamm, pumpen Sie betroffene Räume jedoch erst leer, wenn das Hochwasser abgeflossen und der Grundwasserspiegel ausreichend gesunken ist. Achten Sie auf die Informationen Ihrer Gemeinde.
- Fußbodenbeläge und Verkleidungen sollten Sie zur Kontrolle entfernen oder öffnen.
- Trocknen Sie betroffene Bereiche schnellstmöglich, um Bauschäden, Schimmelpilzbefall oder anderem Schädlingsbefall entgegenzuwirken. Heizgeräte können den Trocknungsvorgang unterstützen.
- Lassen Sie beschädigte Bausubstanz überprüfen (Statik).
- Nehmen Sie elektrische Geräte und Anlagen erst nach Überprüfung durch den Fachmann wieder in Betrieb.
- Lassen Sie Heizöltanks auf Schäden überprüfen.
- Bei Freisetzung von Schadstoffen, wie zum Beispiel Pflanzenschutzmitteln, Farben, Lacken, Reinigern oder Heizöl, verständigen Sie die Feuerwehr. Die Entsorgung ist gegebenenfalls über Fachfirmen erforderlich.
- Benutzen Sie bei Freisetzung von Ölen Ölbindemittel nur in Absprache mit der Feuerwehr.
- Räume, in denen gearbeitet wird, sollten Sie stets gut belüftet halten. Bei freigesetzten Schadstoffen nicht rauchen und offenes Feuer vermeiden.
- Entsorgen Sie verunreinigte Möbel und Lebensmittel.
- Verständigen Sie bei mit dicken Ölschlammschichten bedeckten Gärten oder Feldern das Landratsamt oder Amt für Landwirtschaft.

Über die zuständigen Behörden Ihrer Gemeinde und die Feuerwehr erhalten Sie Informationen, Hinweise und gegebenenfalls die Anschriften von Fachbetrieben.

Tipp: Informationen zum Verhalten bei Hochwasser und bei allen anderen Gefahren können Sie über das deutsche Notfallvorsorge-Informationssystem deNIS erhalten: www.denis.bund.de.

Energieausfall

Alle Bürger der Industrienationen sind heute abhängig von unterschiedlichen Energiequellen. Hierzu gehören Strom, Gas, Öl und Fernwärme, die über Verteilernetze ins Haus geliefert werden. Wie abhängig man von dieser Versorgung ist, zeigen schon die Konsequenzen, die ein Stromausfall mit sich bringen kann. Alle netzbetriebenen Geräte fallen aus. Hierzu können gehören:
- Warmwasserbereiter
- Radio
- Licht

- Bankautomat
- Telefon
- Computer
- stromabhängige Tür- und sonstige Mechanismen
- und viele andere Dinge.

Selbst Heizungen sind vielfach abhängig von Elektrizität, auch die Ölheizung, denn der Transport des Öls durch Steigleitungen, Einspritzung und Zündung funktionieren durch Strom. Diese Funktionen können, wenn überhaupt, nur durch erhebliche und kostspielige Umbauten von Hand gesteuert werden.

Tipps zum Energievorrat:
Falls Öl-, Gas-, Fernwärme- oder Stromversorgung ausfallen, sollte jeder Haushalt alternative Möglichkeiten für diesen Notfall bereithalten. Die fehlende Heizung kann in unseren Regionen über einen gewissen Zeitraum meist durch warme Kleidung ersetzt werden. Wer eine Heizmöglichkeit hat, die auch mit Kohle, Briketts oder Holz betrieben werden kann, sollte für den Notfall diese Brennstoffe bevorraten.

Bei Ausfall des elektrischen Lichtes kann man sich mit Kerzen, Taschenlampen oder Petroleumlampen behelfen. In jedem Fall müssen auch hier die Vorräte an Kerzen, Brennstoffen, Ersatzbirnen für Taschenlampen, Batterien und Zündmittel wie Streichhölzer oder Feuerzeuge überprüft werden. Für einen Notvorrat sind Akkus weniger geeignet, da sie in geladenem Zustand den gespeicherten Strom nicht lange genug halten. Bei Stromausfall müssten sie aber vollständig geladen sein. Bedenken Sie, dass ein Energieausfall unter ungünstigen Umständen auch über mehrere Wochen anhalten kann.

Selbstschutz im Haus

Wenn es auch keinen absoluten Schutz vor allen Schadensfällen gibt, so kann man doch gegen die meisten Gefahren vorbeugen oder durch sinnvolles Handeln schädliche Auswirkungen mildern. So ist es besonders wichtig, sich frühzeitig über eventuell drohende Gefahren an seinem Wohnort und über die dort getroffenen Vorsorgemaßnahmen zu informieren.

Auch in einem Haus können durch Maßnahmen des vorbeugenden Brandschutzes, zum Beispiel durch Verwendung schwer brennbarer Baustoffe, Feuerschutztüren in Heizungskellern, Anbringen von Rauchmeldern sowie durch bereitgehaltene Geräte zur Brandbekämpfung, die Gefahren für Menschen und Sachwerte entscheidend verringert werden.

Möglichkeiten der Brandbekämpfung

Allein durch Brände sterben jährlich bundesweit etwa 600 Menschen, über 5.000 werden verletzt! Allein in privaten Haushalten gehen jährlich Sachwerte in Höhe von über 10 Milliarden Euro in Flammen auf. Bei Katastrophen kann es zu ausgedehnten Bränden kommen. Daher gehört auch der Brandschutz zu den notwendigen Vorsorgemaßnahmen. Kommt es trotz aller Vorsicht zu einem Brand und entstehen zum Beispiel infolge einer Katastrophe sogar viele Brandherde, kann die Feuerwehr nicht gleichzeitig überall sein. Dann kommt es auf schnelles und richtiges Handeln der Betroffenen an, damit Brände möglichst schon unmittelbar nach ihrer Entstehung gelöscht werden. Dazu werden einige einfache Geräte wie Feuerlöscher oder Gartenschlauch benötigt, die gut erreichbar aufbewahrt werden sollten.

Bevor es brennt:
Gleichgültig, ob Sie sich im eigenen Wohnhaus oder einem anderen Gebäude aufhalten, sollten Sie sich vor einem möglichen Brandausbruch darüber informieren
- wie im Gefahrenfall das nächste Treppenhaus zu erreichen ist (diese Treppenhäuser sind Flucht- und Rettungswege, die ins Freie führen; Fahrstühle dürfen im Brandfall nicht benutzt werden),

- welche vorbereitenden Maßnahmen zur Evakuierung gehbehinderter Personen getroffen worden sind,
- welche Möglichkeiten es gibt, den Notruf abzusetzen,
- wo sich Feuerlöschgeräte befinden und wie sie zu bedienen sind.

Bitte beachten Sie,

- dass Flure und Treppenhäuser nicht durch Gegenstände eingeengt oder gar versperrt werden – der Fluchtweg muss ungehindert genutzt werden können,
- dass Türen in Rettungswegen geschlossen aber niemals abgeschlossen werden, um eine Brandausweitung oder Verqualmung des Fluchtweges zu erschweren,
- dass Hydranten oder Feuerwehrzufahrten nicht blockiert sind,
- dass die Sicherheitseinrichtungen des Hauses nicht beschädigt werden und Schäden sofort gemeldet werden,
- dass offenes Licht wie Kerzen oder Feuer immer unter Aufsicht unterhalten wird,
- dass die elektrischen Anlagen und Einrichtungen in einwandfreiem Zustand sind und nicht manipuliert werden,
- dass zu Hause die wichtigsten Dokumente und Papiere griffbereit sind, falls es zu einer überraschenden „Evakuierung“ kommt.

Tipps zur Brandverhütung:

- Im Keller: Leicht brennbares, überflüssiges Material entfernen.
- Auf dem Dachboden: Entrümpeln, insbesondere brennbares Material aus allen Ecken oder unter der Dachschräge entfernen.
- Für den Notfall Löschmittel bereitstellen, zum Beispiel Feuerlöscher, Wasserschlauch, Löschdecke usw.
- Feuerlöscher regelmäßig warten und prüfen lassen.
- Lernen, Löschgeräte zu bedienen und vorhandene Löschmittel richtig einzusetzen.
- Offenes Feuer oder ähnliche Gefahrenquellen nie unbeaufsichtigt lassen.

Wenn es brennt:

Um die eigene Rettung oder die anderer Personen in einem Brandfall zu erleichtern, sollten Sie Kenntnisse über das richtige selbstschutzmäßige Verhalten haben. Oberste Priorität hat die Sicherheit der Menschen. Wenn Sie einen Brand entdecken, so sollten Sie folgende Reihenfolge beachten:

1. Ist das Feuer noch im Entstehen begriffen, so unternehmen Sie augenblicklich erste Löschversuche, um es schon „im Keim“ zu ersticken.
   - Löschversuche nur unternehmen, falls diese ohne Selbstgefährdung möglich sind!
   - Brennendes Fett oder andere flüssige Brennstoffe auf keinen Fall mit Wasser löschen!
   - Bei Gefahr durch elektrischen Strom diesen vor Löschbeginn im Gefahrenbereich abschalten!
   - Von unten nach oben und von der Seite zur Mitte hin löschen!
   - Niemals verqualmte Räume betreten. Dort bilden sich tödliche Brandgase. Schließen Sie die Tür und alarmieren Sie die Feuerwehr.
2. Wenn Löschversuche nicht möglich sind: Fenster des Raumes schließen, wenn dies ohne eigene Gefährdung möglich ist, ebenso die Tür des Raumes, in dem es brennt. Hierdurch wird dem Feuer Sauerstoff entzogen.
3. Feuerwehr rufen.
4. Personen warnen und in Sicherheit bringen (auch durch andere).
5. Feuerwehr erwarten (lassen) und einweisen (lassen).
6. Bis die Feuerwehr eintrifft, sollten Sie versuchen, die Brandausweitung zu erschweren. Tür zum Brandraum feucht halten, um Durchbrand zu verzögern oder zu verhindern.
7. Wenn Sie das Gebäude oder die Wohnung, Etage etc. verlassen müssen, darauf achten, dass keine Person zurückbleibt. Türen zu Räumen, in denen es nicht brennt, sollten unverschlossen bleiben, um gegebenenfalls ein schnelles Absuchen zu unterstützen. Brandschutztüren und Brandabschnittstüren sind selbstverständlich geschlossen. Keine Türen abschließen. Bei Räumen oder Fenstern, die nur mit Schlüssel zugänglich sind, Schlüssel für die Einsatzkräfte bereithalten.

8. Außerhalb der Gefahrenzone sollten Sie feststellen, ob alle Hausbewohner in Sicherheit sind, denn bei einer vermissten Person muss die Feuerwehr immer davon ausgehen, dass sich diese eventuell im Gebäude und somit in Gefahr befindet.

Sie sollten auch bei einem Probealarm (zum Beispiel an Ihrer Arbeitsstelle) wie auf ein echtes Feuer reagieren. Wenn Sie eines Tages einen „echten" Feueralarm für eine Probe halten und nicht reagieren, so kann dies Sie und die Einsatzkräfte in Gefahr bringen.

Weitere Informationen erhalten Sie durch Ihre Feuerwehr.

Gefährliche Stoffe – Schutzgrundsätze

In der Industrie, beim Transport gefährlicher Güter und teilweise sogar im eigenen Haushalt besteht die Möglichkeit, dass gefährliche Stoffe freigesetzt werden können. Sei es beim allzu sorglosen Umgang mit Reinigern oder einem Unfall bis hin zu einer Krisensituation, in der uns gesundheitsgefährdende Stoffe vielleicht bedrohen. Radioaktive und giftige chemische Stoffe treten als Gase, Dämpfe und Staubpartikel auf. Bei einer Freisetzung können diese Stoffe je nach Art und Menge zu einer Gefahr für den Menschen werden.

Ob eine Gefahrensituation vorliegt, die besondere Schutzmaßnahmen für den Menschen erfordert, kann der Bürger im Allgemeinen nicht selbst erkennen. Achten Sie dann auf die Verlautbarungen und Empfehlungen der Behörden, die über Rundfunk und Lautsprecheranlagen verbreitet werden. Einige einfache Verhaltensregeln erhöhen den Schutz in bestimmten Gefahrensituationen und können dazu beitragen, eine Gefahr zu reduzieren.

Selbstschutzmäßiges Verhalten bei Gefahr radioaktiver Kontamination:

1. Bei Aufenthalt im Freien:

- Suchen Sie das nächste bewohnte Haus auf.
- Bewegen Sie sich möglichst quer zur Windrichtung, atmen Sie möglichst durch einen Atemschutz, zumindest ein Taschentuch.
- Wenn Sie bereits mit radioaktiven Stoffen in Berührung gekommen sind, wechseln Sie bei Betreten des Hauses Oberbekleidung und Schuhe.
- Lassen Sie verschmutzte Oberbekleidung und Schuhe außerhalb des Wohnbereichs.
- Waschen Sie Gesicht, Haare und Hände gründlich, ebenso Nase und Ohren.
- Befolgen Sie die Hinweise zum Aufenthalt in Gebäuden.

2. Unterwegs im Auto:

- Schalten Sie die Belüftung aus und schließen Sie die Fenster.
- Hören Sie Radio (UKW, Regionalsender) und befolgen Sie die Anweisungen der Behörden und Einsatzkräfte.
- Fahren Sie ansonsten zum nächsten bewohnten Gebäude und beachten Sie dort die Hinweise unter 1.

3. Bei Aufenthalt im Gebäude:

- Bleiben Sie im Gebäude.
- Nehmen Sie gefährdete Passanten vorübergehend auf.
- Informieren Sie – falls erforderlich – andere Hausbewohner.
- Schließen Sie Türen und Fenster.
- Schalten Sie Ventilatoren und Klimaanlage aus, schließen Sie die Lüftungsschlitze der Fensterrahmen.
- Suchen Sie einen Kellerraum oder einen geschützten Innenraum der Wohnung auf, der möglichst keine Außenfenster hat.
- Vermeiden Sie unnötigen Sauerstoffverbrauch durch Kerzen oder Ähnliches.
- Schalten Sie zu Ihrer Information das Radio auf UKW-Empfang eines Regionalsenders oder das Fernsehgerät ein.
- Beachten Sie die Durchsagen der Behörden und Einsatzkräfte.

- Telefonieren Sie nur in Notfällen.
- Benutzen Sie beim Eindringen radioaktiver Partikel vorhandene Atemschutzgeräte, notfalls Mundschutz wie zum Beispiel OP-Maske oder Tücher.

Selbstschutzmäßiges Verhalten bei biologischen oder chemischen Gefahren:

1. Bei Aufenthalt im Freien:

- Suchen Sie das nächste bewohnte Haus auf.
- Bewegen Sie sich möglichst quer zur Windrichtung, atmen Sie möglichst durch einen Atemschutz, zumindest ein Taschentuch.
- Wenn Sie bereits mit gefährlichen Stoffen in Berührung gekommen sind, wechseln Sie bei Betreten des Hauses Oberbekleidung und Schuhe.
- Lassen Sie verschmutzte Oberbekleidung und Schuhe außerhalb des Wohnbereichs.
- Waschen Sie Gesicht, Haare und Hände gründlich, ebenso Nase und Ohren.
- Befolgen Sie die Hinweise zum Aufenthalt in Gebäuden.

2. Unterwegs im Auto:

- Schalten Sie die Belüftung aus und schließen Sie die Fenster.
- Hören Sie Radio (UKW, Regionalsender) und befolgen Sie die Anweisungen der Behörden und Einsatzkräfte.
- Fahren Sie ansonsten zum nächsten bewohnten Gebäude und beachten Sie dort die Hinweise unter 1.

3. Bei Aufenthalt im Gebäude:

- Bleiben Sie im Gebäude.
- Nehmen Sie gefährdete Passanten vorübergehend auf.
- Informieren Sie – falls erforderlich – andere Hausbewohner.
- Schließen Sie Türen und Fenster.
- Schalten Sie Ventilatoren und Klimaanlage aus, schließen Sie die Lüftungsschlitze der Fensterrahmen.
- Suchen Sie einen gut geschützten Innenraum der Wohnung auf, der möglichst keine Außenfenster hat.
- Meiden Sie Keller oder andere niedrig gelegene Räume.
- Vermeiden Sie unnötigen Sauerstoffverbrauch durch Kerzen oder Ähnliches.
- Schalten Sie zu Ihrer Information das Radio auf UKW-Empfang eines Regionalsenders oder das Fernsehgerät ein.
- Beachten Sie die Durchsagen der Behörden und Einsatzkräfte.
- Telefonieren Sie nur in Notfällen.
- Benutzen Sie beim Eindringen giftiger chemischer Stoffe vorhandene Atemschutzgeräte, notfalls Mundschutz wie zum Beispiel OP-Maske oder feuchte Tücher.

Bis zum Eintreffen der organisierten Fachhilfe sollte jeder in der Lage sein, sich selbst und anderen zu helfen. Die erste Hilfe ist ein wichtiger Bestandteil des Selbstschutzes. Hilfsorganisationen geben Ihnen gerne Auskünfte über Ort und Zeit der angebotenen Lehrgänge.

Bevölkerungs- und Katastrophenschutz

Mit dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) leistet der Bund einen wichtigen Beitrag zum Bevölkerungsschutz, der die Potenziale von Bund, Ländern und Kommunen zu einem integrierten Hilfeleistungssystem verknüpft und verzahnt. Zum Leistungspotenzial des Bundes gehören zum Beispiel Zivilschutz-Hubschrauber in der Luftrettung, ABC-Erkundungsfahrzeuge, das Technische Hilfswerk, aber auch die Dienstleistungen des BBK.

Zuständig für den Selbstschutz sind die Gemeinden. Sie werden bei der Wahrnehmung dieser Aufgabe durch das BBK unterstützt. Die Selbsthilfefähigkeit des Einzelnen ist dabei die unverzichtbare Grundlage organisierter Hilfeleistung. Zu Fragen des Bevölkerungsschutzes oder Selbstschutzes wenden Sie sich an das

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)
Deutschherrenstraße 93-95, 53177 Bonn
Telefon: (0 18 88) 5 50-0, Telefax: (02 28) 55 54-4 36
http://www.bbk.bund.de
info@bbk.bund.de

Zur Unterstützung von Rettungsdiensten und Feuerwehren bei besonderen oder herausragenden Schadensfällen wie Großunglücke, technische Katastrophen und Naturkatastrophen, die ein überörtliches Zusammenwirken von Hilfskräften erfordern, unterhalten die Länder den Katastrophenschutz. Mitwirkende Organisationen hierbei sind unter anderem:

- der Arbeiter-Samariter-Bund
- die Deutsche Lebens-Rettungs-Gesellschaft
- das Deutsche Rote Kreuz
- die Feuerwehren
- die Johanniter-Unfall-Hilfe
- der Malteser-Hilfsdienst
- das Technische Hilfswerk.

In einer Notsituation wie beispielsweise einem Unfall können Menschen verletzt werden, die dann auf fremde Hilfe angewiesen sind. In den seltensten Fällen sind sofort Rettungsdienst oder Feuerwehr zur Stelle. Sie müssen erst über den Notruf alarmiert werden. Grundlage jeder organisierten Hilfe ist daher ein funktionierendes und bekanntes Notruf- und Alarmierungssystem. Überall in Deutschland erreichen Sie die Polizei, die Feuerwehr oder den Rettungsdienst kostenfrei über die folgenden Rufnummern:

Polizei: 110
Feuerwehr: 112

Informieren Sie sich aber bitte auch über weitere ortsbezogene Notfall-Rufnummern. Übrigens: Mit Ihrem Handy können Sie auch ohne Karte jederzeit die Notrufnummer 112 anrufen!

Die Zeit bis zum Eintreffen von Rettungsdienst oder Feuerwehr muss durch selbstschutzmäßige Hilfeleistung überbrückt werden. In welcher Reihenfolge dies geschehen sollte, können Sie nachfolgender Aufstellung entnehmen:

1. Sichern Sie, falls nötig, die Schadensstelle ab.
2. Leisten Sie die lebensrettenden Sofortmaßnahmen.
3. Rufen Sie über 112 oder eine der anderen Notrufnummern Hilfe herbei.
4. Zur Meldung gehören
   - Wo ist es geschehen?
   - Was ist geschehen?
   - Wie viele Personen sind verletzt?
   - Welcher Art sind die Verletzungen?
   - Warten Sie auf Rückfragen!
5. Leisten Sie erste Hilfe bis der Rettungsdienst eintrifft.

Handelt es sich um einen Unfall mit einem Gefahrgut-Transporter, so nennen Sie bitte die oberen Zahlen auf der orangefarbenen Warntafel am Fahrzeug.

Wichtige Rufnummern

Polizei 110
Feuerwehr 112
Rettungsdienst
Ärztlicher Notdienst
Notfall Vergiftungen
Apothekenbereitschaft
Stadtwerke

Notfall	Feuer
Wo ist etwas geschehen?	Wo brennt es?
Was ist geschehen?	Was brennt?
Wie viele Verletzte?	Wie viel brennt (Umfang)?
Welcher Art?	Welche Gefahren? (Personen in Gefahr, Gasflaschen gelagert oder Ähnliches?)
WARTEN auf Rückfragen!	WARTEN auf Rückfragen!

IV Anhang 4

Glossar zum Basisschutzkonzept

ABCR/CBRN-Gefahren	Gefahren atomarer, biologischer, chemischer oder radioaktiver Art (chemical, biological, radiological, nuclear).
Ausfallplanung	Vorsorge zur Aufrechterhaltung oder Wiederherstellung von Unternehmensprozessen für den Fall unvorhergesehener Ereignisse oder Störungen.
BOS	Behörden und Organisationen mit Sicherheitsaufgaben (Polizei- und Katastrophenschutzbehörden von Bund und Ländern, Bundeszollverwaltung, Feuerwehren, THW, Hilfsorganisationen).
Business Continuity Management (BCM)	Alle organisatorischen, technischen und personellen Maßnahmen, die zur Fortführung des Kerngeschäfts eines Unternehmens unmittelbar nach Eintritt eines Krisenfalles und zur sukzessiven Fortführung des gesamten Geschäftsbetriebes bei länger andauernden Ausfällen oder Störungen dienen.
DIN 4102	Brandverhalten von Baustoffen, Bauteilen und Sonderbauteilen.
DIN 18106	Anforderungen an und Prüfverfahren für einbruchhemmende Gitter.
DIN 77200	Grundlegende Anforderungen an die Organisation, Personalführung und Arbeitsweise von Sicherheitsdienstleistern.
DIN EN 356	Sicherheitssonderverglasung/Prüfverfahren und Klasseneinteilung des Widerstandes gegen manuellen Angriff.
DIN ENV 1627	Anforderung an und Klassifizierung von einbruchhemmenden Türen und Fenstern.
DIN/VDE 0185	Blitzschutz/Schutz von baulichen Anlagen und Personen.
dirty bomb	Explosion mit konventionellem Sprengstoff, durch die radioaktive Substanzen verbreitet werden („schmutzige Bombe“).

Dominoeffekt	Abfolge von Ereignissen, von denen jedes einzelne Ereignis zugleich Ursache für das nachfolgende ist; alle Ereignisse sind auf ein und dasselbe Anfangsereignis zurückzuführen.
Elementarschäden	Schäden aus Naturereignissen (zum Beispiel Feuer, Hitze, Blitzschlag, Hochwasser, Sturmfluten, Frost, Lawinen, Steinschlag, Erdbeben).
Gefahr	(Konkrete) Auswirkungen von Gefährdungen/Bedrohungen (Naturereignisse, technisches und menschliches Versagen, menschliches Fehlverhalten) auf Kritische Infrastrukturen.
Gefährdung	Möglichkeit eines Ereignisses (Naturereignisse, technisches und menschliches Versagen, menschliches Fehlverhalten), das zur Schädigung von Personen, Sachwerten und Umwelt oder zu sozialen und ökonomischen Störungen führen kann.
Gefahrenanalyse	Verfahren zur Identifikation und Bewertung der Auswirkungen möglicher Ereignisse auf Infrastrukturen, Objekte oder die Bevölkerung, um Schlussfolgerungen für den Schutz ableiten zu können.
Gefährdungsanalyse	Verfahren zur Identifikation und Bewertung von Gebieten, Infrastrukturen und Objekten, die durch mögliche Ereignisse bedroht sein können.
Gefährdungskategorien	Systematisierung einzelner Gefährdungen anhand der auslösenden Ereignisse.
Gefahrenabwehr	Maßnahmen zur Erhaltung oder Wiederherstellung der öffentlichen Sicherheit.
Gefahrenabwehrbehörden	Die für die Gefahrenabwehr zuständigen Behörden (Polizei- und Ordnungsbehörden).
Infrastrukturen, Kritische	Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.[5]
Interdependenzen	Wechselwirkungen oder gegenseitige Beeinflussung verschiedener Kritischer Infrastrukturen untereinander.
ISO-Norm 17799	Internationaler Standard für Informationssicherheit; Anleitung für den Aufbau und das Führen eines Informationssicherheits-Managementsystems (ISMS).
Katastrophe	(Groß-)Schadensereignis natürlichen Ursprungs (Erdbeben, Sturmfluten, Vulkanausbruch etc.) oder durch menschliche Aktivitäten verursacht (Chemieunfall, Flugzeugabsturz, Anschlag etc.), das zu einer gegenwärtigen Gefahr für das Leben oder die Gesundheit einer Vielzahl von Menschen, für die Umwelt oder für sonstige bedeutsame Rechtsgüter führen und von den für die Gefahrenabwehr zuständigen Behörden mit eigenen Kräften und Mitteln nicht angemessen bewältigt werden kann.

[5] Definition Kritischer Infrastrukturen des AK KRITIS im Bundesministerium des Inneren (BMI) vom 17.11.2003.

Krise

Eine vom Normalzustand abweichende, sich plötzlich oder schleichend entwickelnde Lage, die durch ein Risikopotenzial gekennzeichnet ist, das Gefahren und Schäden für Leib und Leben von Menschen, bedeutende Sachwerte, schwerwiegende Gefährdungen des politischen, sozialen oder wirtschaftlichen Systems in sich birgt und der Entscheidung – oftmals unter Unsicherheit und unvollständiger Information – bedarf.

Krisenkommunikation

Alle kommunikativen Aktivitäten, die in Zusammenhang mit einer Krise durchgeführt werden. In der Praxis bedeutet Krisenkommunikation die klare Zuordnung von Zuständigkeiten und Verantwortlichkeiten sowie eine klare Kommunikationslinie für ein inhaltlich und argumentativ einheitliches Auftreten. Dazu bedarf es auch der Einigung darüber, wie die Medien bei der Aufarbeitung der Krise eingebunden werden sollen.

Krisenmanagement

Schaffung von konzeptionellen, organisatorischen und verfahrensmäßigen Voraussetzungen, die eine schnellstmögliche Zurückführung der eingetretenen außergewöhnlichen Situation in den Normalzustand unterstützen.

Kritikalität

Einschätzung von Umfang und Wahrscheinlichkeit des Ausfalls eines Kritischen Infrastrukturbereichs oder Prozesses.

Notfallplanung

Alle konkreten Vorbereitungen für den Krisen- oder Katastrophenfall, die zu treffen sind, um dessen effektive Bewältigung zu gewährleisten.

Qualitätsmanagement

Alle Maßnahmen eines Unternehmens, die der Schaffung, Sicherung und Verbesserung der Qualität dienen. Umfang und Inhalte des Qualitätsmanagements sind häufig in einem Qualitätsmanagementhandbuch niedergelegt, das sich an den ISO-9000-Normen orientieren sollte. Die Umsetzung des Qualitätsmanagements erfolgt im Unternehmen durch ein entsprechendes Qualitätsmanagementsystem.

Redundanz

Das mehrfache Vorhandensein identischer Ressourcen zum Zweck der Erhöhung der Ausfallsicherheit eines Systems.

Risiko

Erwartung einer ernsten Gefahr, durch die

- das Leben von Menschen bedroht wird,
- die Gesundheit einer großen Zahl von Menschen beeinträchtigt wird,
- wirtschaftliche Aktivitäten, öffentliche Dienstleistungen und technische Infrastrukturen betroffen sind, die Umwelt, insbesondere Tiere und Pflanzen, der Boden, das Wasser, die Atmosphäre sowie Kultur- und Sachgüter geschädigt werden können.

Die Risikoerwartung wird abgestuft dargestellt und mit „sehr hoch“, „hoch“, „mittel“, „niedrig“, „gering“ und „sehr gering“ bezeichnet. Sie ist abhängig von der Anfälligkeit des betrachteten Gebietes gegenüber schädlichen Einwirkungen zum Beispiel natürlicher, physischer, technischer, ökonomischer Art (Vulnerabilität) und der Eintrittswahrscheinlichkeit einer außergewöhnlichen Situation.

	Im mathematischen Sinne wird das Risiko R als Produkt aus der Höhe des Schadens S und der Eintrittswahrscheinlichkeit W bezeichnet: $R = S \times W$
Risikoanalyse	Erfassung des Gefährdungspotenzials und der Anfälligkeit des betrachteten Gebietes oder Objektes gegenüber schädlichen Einwirkungen und Ermittlung der daraus zu folgernden Konsequenzen (Risikobestimmung).
Risikobewertung/-abschätzung	Verfahren der rationalen Urteilsfindung über ein Risiko mit Blick auf dessen Zumutbarkeit für die Gesellschaft als Ganzes oder für bestimmte Gruppen oder Individuen. Bestandteil der Risikobewertung ist die wissenschaftliche Risikoanalyse und die durch empirische Studien erfasste Risikowahrnehmung.
Risikomanagement	Gesamtheit der Maßnahmen zur Minimierung der Risikolage unter Abwägung strategischer Alternativen (Handlungsoptionen) in Konsultation mit den Beteiligten und unter Berücksichtigung der Risikobewertung sowie anderer berücksichtigungswerter Faktoren.
Risikowahrnehmung	Weitgehend auf persönlichen Erfahrungen, vermittelten Informationen und intuitiven Einschätzungen beruhende Risikoabschätzung.
Schaden	Zerstörung und Minderung von konkreten oder abstrakten Werten. Dazu gehören gesundheitliche Beeinträchtigungen, Einbußen an Lebenschancen und Lebensqualität sowie Verlust von geldwerten Gütern. In diese Kategorie fallen auch Formen der ideellen Schädigung, wie beispielsweise der Verlust des Vertrauens in die Integrität politischer Entscheidungsträger.
Schutzziel	Beschreibung eines herbeizuführenden Sollzustands. Schutzziele werden aus den Ergebnissen der Gefährdungsanalyse und der Risikobewertung abgeleitet.
StörfallV	Störfallverordnung, Umsetzung der Seveso-II-Richtlinie in deutsches Recht; enthält Pflichten für Betreiber von Betriebsbereichen i.S.v. § 3 Abs. 5 a Bundesimmissionsschutzgesetz zur Verhinderung von und für das Verhalten nach Störfällen.

Anhang 5

Weiterführende Hinweise

Die nachfolgenden Hinweise auf Literatur, Handbücher und Leitfäden sowie Internetadressen sind als erste Handreichung gedacht und stellen lediglich eine Auswahl aus dem mittlerweile unüberschaubaren Angebot an gedruckter und elektronischer Information dar.

Zur Aktualisierung und Ergänzung insbesondere der Internetversion werden zusätzliche Literaturempfehlungen und weitere Hinweise gerne aufgenommen, entsprechende Angaben werden erbeten an: BBK-Zentrum-I@bbk.bund.de

1. Literatur

Bundesamt für Sicherheit in der Informationstechnik:
IT-Grundschutzhandbuch (Stand: November 2004)
http://www.bsi.bund.de/gshb/deutsch/index.htm

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (Hrsg.):
Vollzugshilfe zur Störfall-Verordnung, März 2004
http://www.umweltministerium.de/files/broschueren/faltblaetter/application/pdf/vollzugshilfe_stoerfall_vo.pdf
(Die Vollzugshilfe zur Störfall-Verordnung kann analog auch auf Unternehmen übertragen werden, die nicht der Störfall-Verordnung unterliegen.)

Bundesministerium für Wirtschaft und Arbeit:
Geheimschutzhandbuch – Handbuch für den Geheimschutz in der Wirtschaft, 2005
https://www.bmwa-sicherheitsforum.de/geheimschutz/ghb.php

Bundesministerium für Wirtschaft und Arbeit:
Leitfaden zum vorbeugenden personellen Sabotageschutz im nichtöffentlichen Bereich, Stand: 14.01.2005
https://www.bmwa-sicherheitsforum.de/shb/ghb/archiv/leitfaden_14.01.05.pdf

Bundesverband deutscher Banken:
Management von Kritischen Infrastrukturen, 2004
http://www.bankenverband.de/pic/artikelpic/052004/br0405_rb_infrastruktur.pdf

Casavant, David:
Emergency Preparedness for facilities. A Guide to Safety Planning and Business Continuity, Maryland, USA 2003

Deloitte:
Erfolg in der Secure Economy – Wachstum und Wohlstand in einer sicheren Wirtschaft. Executive Summary, 2004
http://www.deloitte.com/dtt/cda/doc/content/de_public_Secure_Economy_1204.pdf

Ehses, Herbert u.a. (Hrsg.):
Unternehmensschutz. Praxishandbuch Werksicherheit, Loseblattausgabe, Stuttgart, Stand: Mai 2004

Störfallkommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit:
Leitfaden – Maßnahmen gegen Eingriffe Unbefugter der ad hoc- Arbeitsgruppe „Eingriffe Unbefugter", (SFK-GS-38), 23.10.2002
http://www.sfk-taa.de/berichte_reports/berichte_sfk/sfk_gs_38.pdf

Störfallkommission beim Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit:
Leitfaden für die Darlegung eines Konzepts zur Verhinderung von Störfällen gem. § 8 in Verbindung mit Anhang III der Störfall-Verordnung 2000 für Betriebsbereiche, die den Grundpflichten der Störfall-Verordnung 2000 unterliegen, bearbeitet vom Arbeitskreis MANAGEMENTSYSTEME der SFK (SFK-GS-23, Revision 1), 22.05.2002
http://www.sfk-taa.de/berichte_reports/berichte_sfk/sfk_gs_23_rev1.pdf
(Die Hinweise der Störfallkommission können analog auch auf Unternehmen übertragen werden, die nicht der Störfall-Verordnung unterliegen.)

2. Internetadressen

a) Behörden:
Bundesministerium des Innern: **http://www.bmi.bund.de**
Bundesministerium für Wirtschaft und Arbeit: **http://www.bmwa.bund.de**
Bundesministerium für Verkehr, Bau- und Wohnungswesen: **http://www.bmvbw.bund.de**
Bundesministerium für Gesundheit und soziale Sicherung: **http://www.bmgs.bund.de**
Bundesministerium der Finanzen: **http://www.bundesfinanzministerium.de**
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK): **http://www.bbk.bund.de**
Bundeskriminalamt (BKA): **http://www.bka.de**
Bundesamt für Sicherheit in der Informationstechnik (BSI): **http://www.bsi.bund.de**
Bundesanstalt Technisches Hilfswerk (THW): **http://www.thw.bund.de**
Deutscher Wetterdienst (DWD): **http://www.dwd.de**
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen:
http://www.bundesnetzagentur.de
(vormals: Regulierungsbehörde für Telekommunikation und Post (RegTP))

b) Sonstiges:
Arbeitsgemeinschaft für Sicherheit der Wirtschaft e. V.: **http://www.asw-online.de**
Deutsches Notfallvorsorge-Informationssystem – deNIS: **http://www.denis.bund.de**
Kompetenzzentrum GeoRisikoForschung der Münchner Rückversicherungs-Gesellschaft:
http://www.munichre.org (Topics und Solutions)
Sicherheitsforum: **https://www.bmwa-sicherheitsforum.de**
TSM – System zur Überprüfung der Organisations- und technischen Sicherheit: **http://www.dvgw.de**
Verband der Elektrizitätswirtschaft (VDEW): **http://www.strom.de**
Verband der Netzbetreiber: **http://www.vdn-berlin.de**
Allgemeine Informationen zur Ernährungsvorsorge: **www.ernaehrungsvorsorge.de**

Impressum

Herausgeber:
Bundesministerium des Innern
Referat P II 1
Alt-Moabit 101 D
10559 Berlin
www.bmi.bund.de

Redaktion:
Bundesamt für Bevölkerungsschutz und Katastrophenhilfe,
Zentrum Schutz Kritischer Infrastrukturen (KRITIS) und
Bundeskriminalamt, Referat KI 21

Gesamtgestaltung:
MEDIA CONSULTA Deutschland GmbH,
Sylvia Müller (Kreation),
Dörte Hansen (Redaktion),
Patrick Pabst (Produktion)

Bildnachweis:
Getty Images, picture-alliance

Druck:
Bonifatius GmbH

2. Auflage (November 2005)
10.000 Exemplare

Die Broschüre kann kostenlos bestellt werden.
Publikationsversand der Bundesregierung
Postfach 48 10 09
18132 Rostock
Telefon: 0 18 88 - 8 08 08 00
Telefax: 0 18 88 - 1 08 08 08 00
E-Mail: publikationen@bundesregierung.de

Ihre zum Versand der Publikationen angegebenen personenbezogenen Daten werden nach erfolgter Lieferung gelöscht.